PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10, 7/08

A1

(11) Numéro de publication internationale: WO 99/62037

(43) Date de publication internationale: 2 décembre 1999 (02.12.99)

(21) Numéro de la demande internationale: PCT/FR99/01202

(22) Date de dépôt international: 20 mai 1999 (20.05.99)

(30) Données relatives à la priorité:
98/06450 22 mai 1998 (22.05.98) FR

(71) Déposant: ACTIVCARD [FR/FR]; 24–28, avenue du Général de Gaulle, F–92156 Suresnes Cedex (FR).

(72) Inventeur: AUDEBERT, Yves, Louis, Gabriel; 15–433 Kennedy Road, Los Gatos, CA 95032 (US).

(74) Mandataire: CABINET DE BOISSE ET COLAS; 37, avenue Franklin D. Roosevelt, F–75008 Paris (FR).

(81) Etats désignés: AU, CA, JP, MX, SG, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

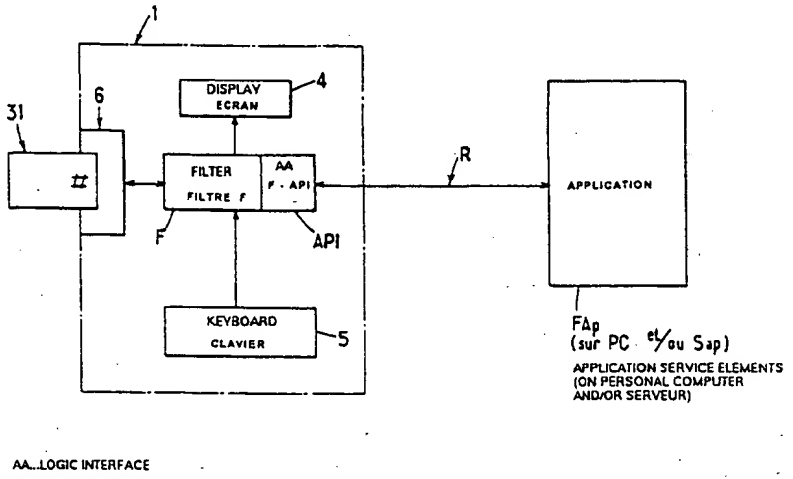
Publiée
Avec rapport de recherche internationale.

(54) Title: TERMINAL AND SYSTEM FOR IMPLEMENTING SECURE ELECTRONIC TRANSACTIONS

(54) Titre: TERMINAL ET SYSTEME POUR LA MISE EN OEUVRE DE TRANSACTIONS ELECTRONIQUES SECURISEES

(57) Abstract

The invention concerns a terminal comprising a terminal module (1) and a personal security device (31). The terminal (1) is adapted for receiving requests from an application (Fap) implanted on an electronic unit in the form of high level requests independent of the module (1) and of said personal security device (31). One at least of the terminal module (1) and the personal security device (31) comprises a reprogrammable storage memory and means for executing a filter software (F) translating the high level requests into at least one of (i) at least one data exchange sequence between the terminal module (1) and the user or (ii) at least an elementary command or sequence of commands executable by the personal security device, and means for protecting said filter software (F, 62) to prevent any modification of said software by a non–authorised person. The filter software comprises means for identifying and/or authenticating the origin of requests transmitted by said application (Fap) implanted in said unit.



(57) Abrégé

Ce terminal comprend un module terminal (1) et un dispositif personnel de sécurité (31). Le terminal (1) est adapté pour recevoir des requêtes d'une application (Fap) implantée sur une unité électronique sous la forme de requêtes de haut niveau indépendants du module (1) et dudit dispositif personnel de sécurité (31). L'un au moins du module terminal (1) et du dispositif personnel de sécurité (31) comprend une mémoire reprogrammable de stockage et des moyens d'exécution d'un logiciel filtre (F) traduisant les requêtes de haut niveau en au moins l'une de (i) au moins une séquence d'échange de données entre le module terminal (1) et l'utilisateur ou (ii) au moins une commande élémentaire ou une séquence de commandes élémentaires exécutables par le dispositif personnel de sécurité, ainsi que des moyens de protection dudit logiciel filtre (F, 62), pour empêcher toute modification dudit logiciel par une personne non autorisée. Le logiciel filtre comprend des moyens d'identification et/ou d'authentification de l'origine des requêtes émises par ladite application (Fap) implantée dans ladite unité.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie
AM	Arménie
AT	Autriche
AU	Australie
AZ	Azerbaïdjan
BA	Bosnie-Herzégovine
BB	Barbade
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BJ	Bénin
BR	Brésil
BY	Bélarus
CA	Canada
CF	République centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire
CM	Cameroun
CN	Chine
CU	Cuba
CZ	République tchèque
DE	Allemagne
DK	Danemark
EE	Estonie
ES	Espagne
FI	Finlande
FR	France
GA	Gabon
GB	Royaume-Uni
GE	Géorgie
GH	Ghana
GN	Guinée
GR	Grèce
HU	Hongrie
IE	Irlande
IL	Israël
IS	Islande
IT	Italie
JP	Japon
KE	Kenya
KG	Kirghizistan
KP	République populaire démocratique de Corée
KR	République de Corée
KZ	Kazakstan
LC	Sainte-Lucie
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LS	Lesotho
LT	Lituanie
LU	Luxembourg
LV	Lettonie
MC	Monaco
MD	République de Moldova
MG	Madagascar
MK	Ex-République yougoslave de Macédoine
ML	Mali
MN	Mongolie
MR	Mauritanie
MW	Malawi
MX	Mexique
NE	Niger
NL	Pays-Bas
NO	Norvège
NZ	Nouvelle-Zélande
PL	Pologne
PT	Portugal
RO	Roumanie
RU	Fédération de Russie
SD	Soudan
SE	Suède
SG	Singapour
SI	Slovénie
SK	Slovaquie
SN	Sénégal
SZ	Swaziland
TD	Tchad
TG	Togo
TJ	Tadjikistan
TM	Turkménistan
TR	Turquie
TT	Trinité-et-Tobago
UA	Ukraine
UG	Ouganda
US	Etats-Unis d'Amérique
UZ	Ouzbékistan
VN	Viet Nam
YU	Yougoslavie
ZW	Zimbabwe

Terminal et système pour la mise en œuvre de transactions électroniques sécurisées

La présente invention concerne un terminal et un système pour la mise en œuvre de transactions électroniques sécurisées.

Les réseaux publics de transmission de données numériques, tels que le réseau Internet, connaissent un développement considérable. Cependant, l'un des freins qui limitent actuellement la mise en œuvre de transactions électroniques sécurisées sur ce type de réseau réside dans l'insuffisance des mécanismes de sécurité associés à de telles transactions, insuffisance qui se traduit par un manque de confiance des utilisateurs et opérateurs de réseaux.

Au sens de la présente demande :

- une transaction électronique désigne un échange d'informations, via un réseau public de transmission de données numériques ou de télécommunications, soit entre deux ou plusieurs utilisateurs, soit entre un utilisateur et un fournisseur de services,
- une fonction est un traitement effectué dans l'objectif de rendre un service à un utilisateur,
- une application désigne un ensemble cohérent de services et de fonctions,
- l'expression logiciel d'application désigne le ou les logiciels nécessaires pour mettre en œuvre les fonctions relatives à une application donnée,
- une transaction sécurisée est une transaction pour laquelle certaines mesures de sécurité sont prises, à savoir l'authentification des entités participant à la transaction, l'intégrité, la confidentialité, l'authenticité, et éventuellement la non répudiation des échanges et opérations effectuées dans le cadre de la transaction.

De nombreuses applications nécessitent que les transactions électroniques mises en œuvre soient sécurisées. Il s'agit par exemple du contrôle d'accès à des ressources informatiques ou similaires, de la banque à domicile (consultation, mouvements de comptes bancaires, etc... par l'intermédiaire du réseau téléphonique ou d'Internet), du commerce électronique (achat de biens ou services par l'intermédiaire d'un réseau public), du courrier électronique, du porte-monnaie électronique, etc...

Ces applications, ainsi que d'autres, nécessitant des transactions sécurisées sont bien connues des spécialistes de la technique et ne sont pas décrites ici en détails.

Suivant leur nature, la sécurisation de ces applications nécessite la mise en œuvre d'un ou plusieurs services de sécurité tels que :

- l'authentification, qui permet de garantir l'identité d'une entité (une personne ou un système) ;
- le contrôle d'accès, qui confère une protection contre l'utilisation ou la manipulation non autorisée de ressources ;
- la confidentialité, qui interdit la divulgation de données à des entités non autorisées ;

- l'intégrité de données, qui assure que des données n'ont pas été modifiées, supprimées ou substituées sans autorisation ;

- la non répudiation, qui assure qu'un participant à un échange de données ne pourra pas ultérieurement nier l'existence de cet échange.

La combinaison de deux techniques existantes permet d'envisager la mise en œuvre de ces services de sécurité, offrant ainsi un niveau de sécurité suffisant pour effectuer des transactions électroniques.

Il s'agit de :

- la cryptographie à clé publique et clé privée, car elle permet de garantir la non répudiation et facilite la gestion des clés ;

- la carte à circuit intégré (ou "smart card") car elle est peu coûteuse, facile à utiliser et sûre grâce à des microprocesseurs spécifiques dotés de protections matérielles et logicielles permettant d'interdire l'accès en lecture et en écriture à leurs mémoires.

Les cartes à circuit intégré offrent les services suivants :

* l'authentification du porteur ou utilisateur de la carte : cette opération permet d'authentifier le porteur à l'aide d'un code confidentiel et à la carte d'accepter par la suite la mise en œuvre d'opérations telles que l'exécution d'algorithmes, la lecture de clés secrètes, la lecture et/ou l'écriture de données dans la carte, qui peuvent en outre être soumises à d'autres conditions de sécurité ;

* la protection des données et fonctions stockées sur la carte à circuit intégré. L'accès à la carte peut être soumis à une authentification préalable de l'entité électronique demandant à y accéder. Cette authentification externe se fait généralement en mode challenge/réponse. Dans ce cas, l'entité dispose d'un paramètre secret, ci-après appelé également secret, qui lui permet de calculer, en fonction d'un challenge émis par la carte, une réponse qui prouvera à la carte qu'elle est en possession du secret ;

* exécution d'algorithmes cryptographiques utilisant un paramètre secret mémorisé dans la carte (chiffrement, authentification de message, signature) ;

* authentification interne. Ce service permet à une application d'authentifier la carte. Ce service est l'inverse d'une authentification externe. La carte génère une réponse en fonction d'un challenge reçu et d'un secret stocké dans la carte.

Les services offerts par la carte à circuit intégré sont mis en œuvre sur réception de commandes dites élémentaires, l'exécution de la commande élémentaire provoquant l'envoi de réponses élémentaires. Ces commandes élémentaires concernent, par exemple, des calculs cryptographiques, la lecture ou l'écriture de données secrètes ou non, des interventions de l'utilisateur (saisie de son code confidentiel personnel PIN, validation d'une

transaction après signature), les retours d'information vers l'utilisateur (affichage des messages à signer, par exemple).

Certaines cartes offrent la possibilité de vérifier l'intégrité, l'origine, voire la confidentialité des commandes envoyées à la carte. Ces services reposent sur des techniques d'authentification et de chiffrement des commandes.

L'utilisation qui est faite actuellement des cartes à circuit intégré (ou cartes à micro-circuit) offre un degré très élevé de sécurité car les transactions sont essentiellement mises en œuvre sur des réseaux privés et des terminaux (distributeurs automatiques de billets, terminaux points de vente par exemple) qui sont sous le contrôle d'une entité assurant la sécurité de l'ensemble du système.

Dans de telles applications, les utilisateurs ou d'éventuels fraudeurs n'ont pas accès au logiciel d'application, ni aux mécanismes de sécurité matériels et logiciels dont sont dotés les terminaux.

Par contre, la mise en œuvre de transactions sécurisées avec des cartes à circuit intégré sur un réseau public suppose que les utilisateurs aient à leur disposition un module terminal lecteur de carte, étant donné que ces cartes à micro-circuit ne sont pas dotées d'une source d'énergie électrique propre et que leur mise en œuvre requiert un lecteur susceptible de les alimenter et d'établir une communication avec l'utilisateur et/ou des moyens électroniques extérieurs.

A l'heure actuelle, pour réaliser une transaction sur un réseau public, l'utilisateur dispose d'un terminal, qui peut être un produit dédié, un ordinateur personnel, ou un ordinateur personnel couplé à une carte à circuit intégré par un lecteur de carte.

Dans tous les cas, le système de transactions à la disposition de l'utilisateur est en général constitué de :

- un fournisseur de services applicatifs pouvant être, par exemple, un navigateur Internet, un logiciel de messagerie, un logiciel de banque à domicile ("Home banking"),
- un fournisseur de services de sécurité de haut niveau permettant l'exécution des mécanismes cryptographiques de bas niveau requis par l'application.

Le fournisseur de services applicatifs émet des requêtes de services de sécurité de haut niveau pour assurer la sécurité des transactions mises en œuvre.

Dans le cas où l'application est implantée sur l'ordinateur personnel de l'utilisateur, les services cryptographiques auxquels il est fait référence sont, par exemple, ceux définis par la Société RSA Laboratories dans son standard "PKCS 11 : Cryptographic Token Interface Standard", ou encore les services cryptographiques offerts par le système d'exploitation Windows NT de Microsoft, en particulier ceux proposés par l'Interface des programmes d'application (API) "Crypto API".

Lorsque l'utilisateur ne dispose pas de lecteur de carte à circuit intégré, les services cryptographiques sont réalisés de manière logicielle uniquement..

Lorsque l'utilisateur veut améliorer la sécurité, il utilise un lecteur de carte à circuit intégré de type transparent connecté a son ordinateur. Un lecteur de carte de type transparent est en fait un boîtier d'interface entre l'ordinateur et la carte à circuit intégré qui permet de transmettre des commandes élémentaires de l'ordinateur, provenant du fournisseur de services cryptographiques, vers la carte, et les réponses élémentaires de la carte vers l'ordinateur. Un utilisateur peut, à l'aide de ce terminal, (constitué de son module terminal - ordinateur + lecteur - couplé à sa carte) effectuer des transactions électroniques (commerce électronique par exemple).

Bien entendu, l'accès des utilisateurs à un tel terminal engendre des risques potentiels du point de vue de la sécurité.

Les risques encourus seront d'autant plus grands que les applications seront décentralisées. Et vice versa, les applications pourront être d'autant plus décentralisées, que les risques côté terminaux seront maîtrisés. Par exemple, on peut envisager des applications de type porte-monnaie, dans lesquelles les transactions (débit de la carte acheteur/crédit de la carte commerçant) se feront de carte à carte, sans nécessiter une consolidation des transactions au niveau d'un serveur central.

Il résulte de ce qui précède, qu'un terminal peut potentiellement contenir un ensemble d'informations, voire des logiciels, sur la confidentialité et l'intégrité desquels repose la sécurité de l'application. Comme exemple, on peut citer des clés secrètes utilisées pour l'authentification du module terminal vis-à-vis de la carte, ou pour le chiffrement de données entre un serveur et le module terminal lecteur de carte. Or, un fraudeur peut profiter du fait d'avoir à sa disposition un terminal pour analyser son fonctionnement et accéder aux informations et logiciels confidentiels.

Il faut également noter que les applications auxquelles il est fait référence ici, telles que le commerce ou le courrier électronique, sont la plupart du temps mises en oeuvre à travers le réseau Internet. Il est bien connu des experts qu'un ordinateur personnel ou PC connecté au réseau Internet est très vulnérable aux logiciels de type virus, qui peuvent être installés et exécutés sur le PC de l'utilisateur sans même qu'il le sache et sans qu'il ait laissé un accès physique à son ordinateur à qui que ce soit. Le côté totalement invisible de ce type de menace représente le réel danger qui limite à l'heure actuelle le déploiement des applications transactionnelles utilisant Internet. Les mêmes commentaires peuvent s'appliquer aux applications de commerce électroniques envisagées à partir des réseaux

câblés de télévision en utilisant des décodeurs ou "set-top box" raccordés au poste de télévision et comportant un ou deux lecteurs de cartes à puce.

Les risques au niveau du système sont alors les suivants :

• Attaque sur l'intégrité du fournisseur de services cryptographiques et du fournisseur de services applicatifs visant à modifier le comportement du module terminal : à titre d'exemple, le module terminal est modifié de manière à capturer les informations liées à la carte, stocker les informations obtenues pour ensuite les communiquer à un faux serveur. Cette attaque peut être réalisée à l'insu de l'utilisateur légitime (substitution du module terminal de l'utilisateur ou prêt d'un module terminal modifié). Cette attaque peut ensuite se généraliser sous la forme de la diffusion de modules terminaux contrefaits ;

• Attaque sur la confidentialité du fournisseur de services cryptographiques, visant à se procurer les clés cryptographiques qu'il manipule, lesquelles clés sont par exemple stockées sur le disque dur d'un ordinateur.

• Attaque vis-à-vis d'autres cartes, basée sur une capacité à pouvoir s'authentifier vis-à-vis de ces cartes, grâce aux secrets découverts par une attaque sur la confidentialité du fournisseur de services.

• Attaque sur l'intégrité et la confidentialité des communications entre les différentes entités (fournisseurs de services applicatifs, fournisseurs de services cryptographiques, lecteur de carte à circuit intégré, carte à circuit intégré, serveur) permettant de rompre la chaîne de confiance établie entre ces éléments . Par exemple:

1 - déchiffrement des communications entre serveur et terminaux ;

2 - insertion d'un logiciel tiers entre le fournisseur de services applicatifs et le fournisseur de services cryptographiques visant à rompre la chaîne de confiance entre ces deux logiciels ou bien substitution du logiciel applicatif par un logiciel tiers visant à faire exécuter au fournisseur de services de sécurité des requêtes de sécurité dans un but différent de celui de l'application connue de l'utilisateur.

• Attaque sur les serveurs (dans le cas d'une application en mode connecté) : connexion d'un terminal contrefait à un serveur, émulation d'un couple module terminal-carte à circuit intégré pour obtenir des avantages.

Ainsi, une attaque sur la chaîne de confiance entre le fournisseur de services cryptographiques et le fournisseur de services applicatifs, dans le cadre d'une application requérant la signature d'une transaction électronique à l'aide d'une carte à circuit intégré, est illustrée ci-après. Le déroulement de la transaction est le suivant :

- Etape 1 : vérification du code confidentiel personnel (PIN) de l'utilisateur, que celui-ci introduit par un clavier associé à son module terminal, le code introduit étant transmis à la carte pour vérification par cette dernière.

- Etape 2 : authentification du module terminal. Ce dernier envoie une commande "demande challenge". (Un challenge est un nombre aléatoire ou pseudo-aléatoire). La carte à circuit intégré génère le challenge et le transmet au module terminal. Le module terminal envoie à la carte une commande "authentification externe" accompagnée d'une réponse constituée du challenge chiffré par une clé détenue par le module terminal. La carte à circuit intégré vérifie alors la réponse reçue.

- Etape 3 : si les étapes 1 et 2 se sont déroulées de manière satisfaisante, la carte à circuit intégré est prête à recevoir et exécuter la commande signature, c'est-à-dire une commande de chiffrement, au moyen d'une clé privée stockée dans la carte, du résultat d'une opération de hachage réalisée sur la transaction saisie par l'utilisateur. Après ce chiffrement, la carte émet, à destination du module terminal, la signature constituée du résultat de l'opération de hachage ("hash") ainsi chiffré.

Si l'intégrité du logiciel d'application (fournisseur de services applicatifs et son fournisseur de services cryptographiques) n'est pas assurée, un fraudeur n'a pas besoin de connaître les clés et codes secrets pour pirater le système de transaction : il lui suffit d'implanter dans le module terminal, par exemple dans l'ordinateur personnel auquel est raccordé un lecteur de carte à circuit intégré, un logiciel de type virus qui, à l'étape 3, détourne les données authentiques à signer et envoie à la carte des données falsifiées. Etant donné que les étapes 1 et 2 se sont déroulées de manière satisfaisante, la carte signera alors les données falsifiées sur la base du PIN que l'utilisateur a lui-même introduit et celui-ci croira que la carte va signer ses propres données.

L'exemple précédant montre la nécessité de protéger non seulement les informations confidentielles mises en oeuvre dans le cadre d'une transaction, mais aussi l'intégrité de la transaction, c'est-à-dire l'intégrité du comportement de chaque entité intervenant dans la transaction, ainsi que l'intégrité du comportement d'ensemble du logiciel en veillant à la non rupture de la chaîne de confiance établie entre les différentes entités.

Les risques d'attaque mentionnés ci-dessus sont à l'heure actuelle en partie couverts par des terminaux - lecteurs de carte à circuit intégré intégrant des modules de sécurité (SAM, analogue à une carte à circuit intégré) qui sont utilisés notamment dans le cadre des applications porte-monnaie. Le lecteur est alors personnalisé par un SAM, et attribué à un commerçant, les cartes lues étant celles des clients. Ce SAM contient des informations secrètes et est susceptible d'exécuter des algorithmes utilisant ces informations secrètes. Mais, il ne contient pas de moyens permettant notamment de piloter les communications avec l'utilisateur, avec la carte à circuit intégré et/ou avec des moyens électroniques extérieurs, et donc la sécurisation de transaction n'est pas assurée.

Il est également connu par le document WO 95/04328 un module terminal comprenant des moyens d'interface avec l'utilisateur et des moyens d'interface avec des moyens électroniques extérieurs (ci-après appelés moyens d'interface externe), comportant une interface avec une carte à micro-circuit. Le microprocesseur du module terminal comprend des moyens de stockage de données (ROM, EEPROM, RAM). Les données stockées en mémoire permanente (ROM) comprennent entre autres un système d'exploitation, des gestionnaires de composants externes pilotant les interfaces et périphériques, et un interpréteur capable d'interpréter des modules programmes écrits dans un langage spécifique. Les modules programmes sont stockés dans la mémoire semi-permanente EEPROM et peuvent être chargés en mémoire temporaire RAM pour être exécutés par le microprocesseur lors de l'activation d'une interface appropriée par l'utilisateur. Les modules programmes, correspondant aux applications du module terminal, sont téléchargés dans la mémoire EEPROM du microprocesseur ou dans une carte à micro-circuit à partir d'un serveur externe.

Le module terminal du document WO95/04328 peut fonctionner :

- en mode module terminal autonome, le microprocesseur du module terminal exécutant un module programme stocké dans une mémoire interne, sans faire appel à une carte à circuit intégré ;
- en mode terminal autonome, dans lequel un module programme stocké dans une carte est exécuté ;
- en mode terminal étendu ou connecté, dans lequel le microprocesseur du module terminal ou celui de la carte exécute un module programme et une communication est établie via le téléphone, un modem ou une liaison directe avec un fournisseur de services ou un serveur ;
- en mode lecteur de carte à mémoire transparent, dans lequel des instructions reçues par une liaison série sont transmises directement à la carte et vice et versa.

Le terminal décrit au document WO 95/04328 ne traite pas des problèmes de sécurité visés par l'invention dans la mesure où il ne décrit pas comment sécuriser une transaction en garantissant l'intégrité du comportement d'ensemble du logiciel exécutant la transaction. Il ne décrit notamment pas de moyens permettant l'exécution de requêtes de haut niveau émises par l'application, ni comment garantir l'origine, l'intégrité et la confidentialité de ces moyens.

La présente invention vise à fournir un terminal pour la mise en œuvre de transactions électroniques sécurisées, du type comprenant un dispositif personnel de sécurité tel qu'une carte à circuit intégré ou autre dispositif remplissant les mêmes fonctions, et un module terminal doté de moyens d'interface avec le dispositif personnel de sécurité, tels qu'un lecteur de carte à circuit intégré, et offrant de par son architecture logicielle et/ou matérielle et les mécanismes de sécurité qu'il comporte, un niveau de sécurité amélioré, compatible

avec le fait que le terminal peut être placé sous le contrôle des utilisateurs, (par opposition à des terminaux contrôlés par des opérateurs).

Un deuxième objectif de l'invention est d'assurer ce même niveau de sécurité tout en permettant l'intégration, en cours d'utilisation, de fonctions ou applications nouvelles, ou l'évolution des fonctions ou applications existantes sans avoir recours à une multitude de modules terminaux différents ou au changement des modules terminaux lors des évolutions.

A cet effet, l'invention a pour objet un terminal pour la mise en œuvre, par un utilisateur, de transactions électroniques sécurisées en liaison avec au moins une application implantée sur une unité électronique, ledit terminal comprenant :

- un module terminal comportant au moins :
  - des premiers moyens d'interface avec ladite application pour en recevoir des requêtes relatives auxdites transactions,
  - des deuxièmes moyens d'interface avec ledit utilisateur,
  - des troisièmes moyens d'interface avec un dispositif personnel de sécurité,
  - des premiers moyens de traitement de données comprenant au moins des premiers moyens logiciels de pilotage desdits moyens d'interface, et

- un dispositif personnel de sécurité comportant au moins des deuxièmes moyens de traitement de données sécurisées comprenant au moins des deuxièmes moyens logiciels d'exécution de commandes élémentaires et des moyens d'exécution de calculs cryptographiques, caractérisé en ce que :

  * ledit terminal est adapté pour recevoir lesdites requêtes de ladite application implantée sur ladite unité électronique sous la forme de requêtes de haut niveau indépendantes dudit dispositif personnel de sécurité,
  * l'un au moins dudit module terminal et dudit dispositif personnel de sécurité comprend :
    - au moins une mémoire reprogrammable de stockage d'au moins un logiciel filtre, traduisant lesdites requêtes de haut niveau en en au moins l'une de :

      (i) au moins une commande élémentaire ou une séquence de commandes élémentaires exécutables par lesdits deuxièmes logiciels desdits deuxièmes moyens de traitement de données, ou

      (ii) au moins une séquence d'échange de données entre ledit module terminal et ledit utilisateur via lesdits seconds moyens d'interface, ledit échange de données étant exécuté par lesdits premiers moyens logiciels desdits premiers moyens de traitement de données,
    - des moyens de protection dudit logiciel filtre pour empêcher toute lecture et/ou modification dudit logiciel par une personne non autorisée, et

* l'un au moins desdits premiers et deuxièmes moyens de traitement de données comprend un dispositif de traitement de données pour l'exécution dudit logiciel filtre.

L'invention définie ci-dessus permet d'atteindre les objectifs de sécurité requis par la mise en oeuvre de transactions électroniques grâce au fait qu'elle décrit un filtre ou pare-feu (" firewall ") entre le monde extérieur, c'est-à-dire les applications elles-mêmes, et les moyens de sécurité et périphériques qu'il gère, au moyen d'une interface logique permettant la définition du format des requêtes de haut niveau émises par les applications et d'un logiciel de traduction assurant le traitement de ces requêtes.

De préférence, le terminal suivant l'invention comprend une ou plusieurs des caractéristiques suivantes, éventuellement combinées :

- ledit dispositif d'exécution du logiciel filtre comprend des premiers moyens d'identification et/ou d'authentification de ladite application implantée dans ladite unité ou de l'origine desdites requêtes émises par ladite application ;
- ledit dispositif de traitement de données pour l'exécution dudit logiciel filtre comprend des moyens de vérification de l'intégrité des données reçue de ladite application ;
- ledit dispositif de traitement de données pour l'exécution dudit logiciel filtre comprend des moyens centralisés de contrôle des conditions d'utilisation des services du dispositif personnel de sécurité, en fonction de ladite application et/ou dudit utilisateur ;
- ledit dispositif de traitement de données pour l'exécution dudit logiciel filtre comprend :
  - des moyens pour commander le chargement sécurisé dudit logiciel filtre dans ladite mémoire programmable, via l'un desdits premiers ou troisièmes moyens d'interface, à partir d'une entité extérieure audit module, et
  - des premiers moyens de contrôle d'accès pour n'autoriser ledit chargement dudit logiciel filtre qu'en réponse à au moins une condition prédéfinie ;
- le terminal comprend des deuxièmes moyens d'authentification desdits premiers moyens de traitement de données par lesdits deuxièmes moyens de traitement de données ;
- le terminal comprend des troisièmes moyens d'authentification desdits deuxièmes moyens de traitement de données par lesdits premiers moyens de traitement de données ;
- le terminal comprend un premier canal de communication entre lesdits premiers et deuxièmes moyens de traitement de données et des premiers moyens de sécurisation dudit premier canal de communication ;
- le terminal comprend des quatrième moyens d'authentification dudit module terminal par ledit utilisateur, indépendamment de ladite carte ;
- lesdits quatrièmes moyens d'authentification comprennent des moyens de calcul, par lesdits premiers moyens de traitement de données, et de présentation audit utilisateur, via

lesdits deuxième moyens d'interface, d'un mot de passe connu dudit utilisateur et calculé sur la base d'au moins un premier paramètre secret stocké dans lesdits premiers moyens de traitement de données ;

- le terminal comprend des cinquièmes moyens d'authentification conjointe dudit module terminal et de ladite carte par ledit utilisateur ;

- lesdits cinquièmes moyens d'authentification comprennent des moyens de calcul, par ledit dispositif d'exécution dudit logiciel, et de présentation audit utilisateur, via lesdits deuxièmes moyens d'interface, d'un mot de passe connu dudit utilisateur et calculé sur la base d'au moins un deuxième et un troisième paramètres secrets stockés respectivement dans lesdits premiers et deuxièmes moyens de traitement de données.

Selon une première forme de réalisation de l'invention, le module terminal est constitué par un ordinateur personnel et ladite mémoire programmable est constituée par le disque dudit ordinateur, ledit logiciel filtre est exécuté sur l'ordinateur personnel ou bien dans un deuxième mode d'exécution, ladite mémoire programmable est implantée sur un serveur sécurisé relié à l'ordinateur personnel, la partie du logiciel filtre devant être protégé étant exécutée sur ledit serveur sécurisé.

Selon une deuxième forme de réalisation de l'invention, le module terminal est un dispositif, tel qu'un lecteur dédié de carte à circuit intégré, auquel cas ledit dispositif personnel de sécurité est une carte à circuit intégré, ou un ordinateur personnel. Ce mode de réalisation se différencie du précédent par le fait que ladite mémoire programmable est intégrée dans un microprocesseur sécurisé, ledit logiciel filtre étant exécuté dans ledit microprocesseur sécurisé. Le module terminal dédié peut éventuellement être portable.

Selon les modes d'exécution de cette deuxième forme de réalisation de l'invention, la mémoire programmable pour le chargement et le stockage du logiciel filtre peut être disposée dans le dispositif personnel de sécurité ou dans le module terminal.

Dans ce dernier cas :

- le module terminal peut comporter un seul microprocesseur pour l'exécution du logiciel filtre et le pilotage des interfaces, ou bien deux microprocesseurs remplissant respectivement l'une et l'autre de ces deux fonctions.

- de préférence ledit logiciel filtre comprend au moins un paramètre secret et lesdits deuxièmes moyens de traitement de données comprennent des seconds moyens de contrôle d'accès conditionnels pour n'autoriser l'exécution desdits calculs cryptographiques, en réponse à des commandes élémentaires générées par ledit logiciel filtre, que si au moins une seconde condition prédéfinie, fonction dudit paramètre secret est remplie

Selon d'autres caractéristiques de l'invention, lorsque le module terminal comporte deux microprocesseurs pour l'exécution du logiciel filtre et le pilotage des interfaces :

- le terminal comprend un deuxième canal de communication entre lesdits premiers moyens logiciels de pilotage des moyens d'interface et ledit deuxième microprocesseur et des deuxièmes moyens de sécurisation dudit deuxième canal de communication ;

- lesdits deuxièmes moyens de sécurisation comprennent des moyens de chiffrement et déchiffrement, par lesdits premiers moyens logiciels de pilotage des moyens d'interface et ledit deuxième microprocesseur, des données transmises sur ledit deuxième canal de communication, sur la base d'au moins un cinquième paramètre secret mémorisé dans lesdits premiers et deuxièmes moyens de traitement de données ;

- lesdits deuxièmes moyens de sécurisation comprennent des premiers moyens physiques de protection dudit deuxième canal de communication contre les intrusions.

Différents modes de réalisation de l'invention seront maintenant décrits en se référant aux dessins annexés, en particulier des modes de réalisation dans lesquels le logiciel filtre est chargé et exécuté dans le terminal de manière à garantir à la fois son origine, sa confidentialité et son intégrité, ce logiciel pouvant aussi authentifier l'origine des requêtes qui lui sont envoyées, si la confiance dans les interfaces avec l'utilisateur, c'est-à-dire l'écran et le clavier, ne peut être garantie.

- la Figure 1 est un schéma illustrant l'architecture fonctionnelle d'un système pour la mise en œuvre de transactions sécurisées au moyen d'un terminal selon l'invention ;

- la Figure 2A présente une première forme de réalisation de l'invention où le terminal est un ordinateur personnel couplé à une carte à circuit intégré par un lecteur, l'application pouvant être elle même implantée sur l'ordinateur personnel ou sur un serveur distant.

- la Figure 2B décrit l'architecture fonctionnelle d'une variante d'exécution de la première forme de réalisation de l'invention, dans laquelle l'ordinateur personnel servant de terminal est en liaison avec un serveur de sécurité sur lequel est implanté le logiciel filtre ;

- la Figure 3 présente un système de transaction mis en oeuvre grâce à un terminal selon une deuxième forme de réalisation de l'invention, qui peut être un produit dédié relié en tant que périphérique à un ordinateur personnel ou directement à un serveur ou bien construit autour d'un ordinateur personnel ;

- la Figure 4A est un schéma bloc de l'architecture matérielle des circuits électroniques d'un premier mode d'exécution du terminal de la figure 3 ;

- la Figure 4B est un schéma fonctionnel illustrant une première configuration d'architecture logicielle du terminal de la figure 4A ;

- la Figure 4C est un schéma fonctionnel similaire à celui de la figure 4B présentant une seconde configuration d'architecture logicielle du terminal de la figure 4A ;

- la Figure 5 est un schéma bloc de l'architecture matérielle des circuits électroniques d'un deuxième mode d'exécution du terminal autonome de la figure 3 ;

- la Figure 6 est un schéma bloc de l'architecture matérielle des circuits électroniques d'un troisième mode d'exécution du terminal autonome de la figure 3 ;

- la Figure 7 est un schéma illustrant l'architecture logicielle conventionnelle d'une carte à micro-circuit ;

- la Figure 8A est un schéma illustrant l'architecture logicielle d'un système de transaction comprenant le terminal de la figure 4A ;

- la Figure 8B est un schéma illustrant l'architecture logicielle d'un système de transaction comprenant le terminal de la figure 6 ;

- la Figure 9 est un diagramme illustrant la mise en œuvre d'une application de commerce électronique au moyen d'un système selon l'invention ; et

- la Figure 10 est un organigramme illustrant le processus de téléchargement d'un programme dans une mémoire reprogrammable du module terminal de la figure 4A ou 5, ou d'une carte à micro-circuit connectée à celui-ci ;

En se référant à la figure 1, un système de mise en œuvre de transactions sécurisées comprend un module terminal 1 de lecture d'une carte à circuit intégré 31 ou équivalent. Le module terminal 1 comprend un filtre F constitué d'un module logiciel traitant des requêtes de haut niveau émises par des fournisseurs de services applicatifs FAp externes au module terminal 1 au moyen d'une interface logique F-API, et des interfaces utilisateur telles qu'un écran d'affichage 4 et un clavier 5 permettant la lecture et l'introduction de données par un utilisateur. Il comprend également un lecteur ou interface de communication 6 avec une carte à micro-circuit ou tout dispositif de sécurité équivalent personnel à l'utilisateur, du type jeton (token), " JavaRing " (produit de la société SUN), " iButton " (produit de la société Dallas Semiconductor Corporation), jeton logiciel (soft token), ainsi que des interfaces de communication avec au moins un fournisseur de services applicatifs FAp qui peut, par exemple, être implanté sur un ordinateur personnel PC et/ou sur un serveur Sap , l'échange de données s'effectuant alors via un réseau R de transmissions de données ou de télécommunications.

Le module terminal 1 peut être un terminal dédié ou être intégré dans un ordinateur personnel de type PC, ou bien dans un ordinateur-terminal NC dédié aux applications en réseau (Network Computer) ou encore dans un décodeur de réseau de télévision câblé (Set Top Box).

Le module terminal 1 peut éventuellement être utilisé en mode autonome, par exemple pour lire des informations, telles que le contenu d'un porte-monnaie électronique, contenues dans une mémoire de la carte 31.

Pour la mise en œuvre de transactions sécurisées, le module terminal 1 peut être utilisé en mode connecté avec un serveur Sap ou en mode non connecté, l'application FAp étant alors exécutée localement, par exemple sur l'ordinateur personnel PC : Tel est le cas, par exemple, lorsqu'un utilisateur doit signer un courrier électronique ou des transactions qui seront envoyées à un destinataire. Une telle opération n'implique pas de connexion avec un serveur applicatif au moment où la carte 31 est utilisée.

En mode connecté, comme représenté à la figure 3 dans le cas d'un module terminal 1 dédié, celui-ci peut être connecté au serveur Sap sur lequel est implanté l'application FAp par l'intermédiaire de l'ordinateur PC et d'un réseau R tel qu'Internet, ou par l'intermédiaire du réseau téléphonique R via un modem MO ou une liaison DTMF avec un combiné téléphonique CT. Certaines transactions, telles que le rechargement d'un porte-monnaie électronique dans la carte 31, peuvent nécessiter un échange bidirectionnel de données avec le serveur Sap et sont, par conséquent, plus ergonomiques en mode connecté.

La mise en œuvre d'une transaction sécurisée avec un module terminal 1 et une carte 31 implique que des requêtes logicielles de haut niveau (par exemple des requêtes de signature, d'authentification , etc... qui doivent être traitées de manière à satisfaire les objectifs de sécurité requis du programme applicatif) soient transmises du programme applicatif implanté par exemple dans le serveur Sap (mode connecté) ou dans l'ordinateur personnel PC ou NC à la disposition de l'utilisateur (mode non connecté, par exemple signature de courrier électronique), au filtre F assurant le pilotage des moyens de sécurité. Ce filtre F effectue le traitement de ces requêtes au moyen d'un logiciel de traduction, s'assurant ainsi que l'application ou tout autre logiciel de type virus ne peuvent avoir un accès direct aux fonctions cryptographiques de la carte à circuit intégré 31. Le traitement des requêtes de haut niveau comprend la traduction de ces requêtes en une commande élémentaire ou une séquence de commandes élémentaires qui sont exécutées par le dispositif personnel de sécurité. Les requêtes de haut niveau sont formulées indépendamment de la configuration matérielle et/ou logicielle du dispositif personnel de sécurité, c'est-à-dire qu'elles ne sont pas formulées directement en fonction du dispositif personnel de sécurité.

Les requêtes de haut niveau contiennent des informations qui sont liées spécifiquement au processus qui sera exécuté par le logiciel filtre. Selon un exemple simple, une requête de haut niveau peut comprendre une commande élémentaire unique à transmettre au dispositif personnel de sécurité, par exemple un APDU ("Application Protocol Data Unit"), dans le cas

d'une carte à microcircuit, attaché à un code MAC d'authentification de message qui permettra au logiciel filtre F de vérifier l'origine et l'intégrité de cette requête avant d'envoyer la commande élémentaire au dispositif personnel de sécurité. Selon un exemple plus complexe, tel qu'une requête de signature d'un document, la requête de haut niveau sera transformée par le filtre F en une séquence de commandes élémentaires envoyées au dispositif personnel de sécurité et éventuellement à l'interface utilisateur. Ainsi, selon cette définition et du fait qu'elles contiennent des informations spécifiques devant être décodées par le filtre F indépendamment du dispositif personnel de sécurité, les requêtes de haut niveau sont dites être indépendantes du dispositif personnel de sécurité.

Le filtre F répond aux objectifs de sécurité recherchés dans la mesure où le logiciel de traduction qu'il comporte vérifie l'identité de l'application émettant les requêtes de services (ou directement l'origine des requêtes) et est implanté de manière à garantir l'intégrité et la confidentialité des opérations et données élémentaires mises en oeuvre pour répondre aux requêtes de services.

Un logiciel de traduction est un logiciel configuré pour un type de carte à micro-circuit et traduit une requête de haut niveau reçue d'un logiciel d'application en une commande élémentaire ou une séquence de commandes élémentaires exécutables par les cartes à micro-circuit et/ou une séquence d'échanges de données avec l'utilisateur.

Les requêtes de haut niveau sont une liste de commandes utilisées par les programmes applicatifs pour faire appel aux services de sécurité nécessaires pour identifier et authentifier la personne réalisant la transaction et garantir l'origine, l'intégrité et éventuellement la non-répudiation de la transaction. Une requête de haut niveau provenant d'une application (se trouvant sur un serveur ou sur l'ordinateur personnel PC ou NC) peut être caractérisée par un ou plusieurs des points suivants :

- elle est indépendante des moyens de base (moyens cryptographiques par exemple) mis en oeuvre pour satisfaire à sa demande et contient des informations spécifiques devant être traitées par le filtre F. Réciproquement, plusieurs applications peuvent utiliser le même fournisseur de services de sécurité, faisant alors appel à la même interface logique F-API définissant ces requêtes.

- le traitement de la requête permet de lier la transaction de manière certaine à l'utilisateur effectuant la transaction à l'aide d'au moins un paramètre secret, fixe ou variable, stocké dans la carte à circuit intégré de l'utilisateur.

- elle comporte éventuellement une information ou des informations permettant au logiciel filtre F de vérifier son origine et son intégrité. L'authentification peut se faire à l'aide

d'un code de type " Message Authentication Code ou MAC " ou bien de type " signature électronique " associé à la requête.

- dans le cas où la transaction n'est pas saisie par l'utilisateur sur le module terminal lui-même, la requête contient éventuellement l'information nécessaire pour permettre à l'utilisateur de vérifier, s'il le souhaite et si le module terminal supporte cette option, les données essentielles de la transaction.

L'interface logique F-API permettant l'échange des requêtes de sécurité de haut niveau entre les applications et le logiciel de traduction du filtre F peut être standardisée de manière à être commune à différents programmes applicatifs. Ainsi, la requête de type " Signature " peut être utilisée par une messagerie électronique ou par un logiciel d'achat. Il est ainsi possible de changer l'application tout en conservant le fournisseur de services de sécurité ou réciproquement de remplacer le fournisseur de services de sécurité sans modifier l'application.

Afin de garantir l'intégrité de la chaîne de confiance entre l'application et la carte, le logiciel filtre F de traduction identifie, voire authentifie l'origine et l'intégrité des requêtes qu'il reçoit. Différentes méthodes peuvent être envisagées pour identifier l'application émettant les requêtes :

- un code d'identification peut être intégré dans la requête elle- même puis vérifié par le logiciel filtre à partir des informations qu'il contient ou qui peuvent être stockées dans la carte à circuit intégré ;

- le même but peut être atteint en comparant le résultat d'une opération de hachage exécuté par le logiciel filtre sur le logiciel applicatif émettant la requête avec un résultat préalablement stocké dans la carte par exemple. Cette dernière solution est particulièrement adaptée au cas où l'application est implantée sur le PC de l'utilisateur ;

- l'authentification peut également être réalisée en associant à la requête un code de type " MAC " calculé à partir du contenu de la requête et d'une clé secrète partagée entre l'application et le logiciel filtre. Un principe équivalent peut être utilisé avec une signature de la requête calculée avec les mêmes informations et une clé privée connue de l'application, la signature étant vérifiée avec la clé publique correspondante connue du logiciel filtre.

La figure 2A décrit une première forme de réalisation pour laquelle le module terminal 1 est un ordinateur personnel PC 102, la liaison avec la carte à circuit intégré 31 s'effectuant au moyen d'un lecteur 6 connecté ou intégré à l'ordinateur PC 102. L'ordinateur personnel 102 comprend des interfaces d'entrée/sortie 102a avec le lecteur 6 et le serveur Sap. Suivant la nature du lecteur connecté au PC, les éléments d'interface avec l'utilisateur peuvent être le clavier et l'écran du PC lui-même, ou bien un clavier et/ou un afficheur de type LCD par exemple implanté sur le lecteur. Dans ce mode de réalisation, le filtre F est implanté et

exécuté sur l'ordinateur PC 102. Le filtre F, et donc le logiciel de traduction qu'il contient, peut alors être stocké sur le disque dur HD 102b de l'ordinateur personnel 102. Pour être exécuté par l'unité de calcul ou microprocesseur 102c du PC, le logiciel filtre est ensuite chargé dans la mémoire vive RAM 102d de l'ordinateur personnel 102.

Le disque dur d'un ordinateur PC étant difficile à protéger, le logiciel filtre F, ou tout au moins la partie sensible de ce logiciel, peut être chiffré. Pour cela il peut être décomposé en au moins 2 modules : un module de chargement/déchiffrement Fcd et un deuxième module correspondant au logiciel filtre lui-même chiffré, Fchi. Le premier module permet le chargement du deuxième module en mémoire RAM, son déchiffrement, puis le lancement de son exécution. En se référant à la Figure 2A, le module logiciel déchiffré et chargé en RAM est nommé Fdec.

L'utilisation d'un langage de programmation tel que Java, par des mécanismes de sécurité intrinsèques au langage lui-même, permet de renforcer la protection du logiciel

Une autre méthode de vérification de l'intégrité du logiciel filtre est de faire signer le deuxième module par une autorité garante du contenu du logiciel filtre au moyen d'une clé privée conservée secrète par cette autorité. Le premier module de chargement effectue alors, simultanément à l'opération de déchiffrement, une opération de hachage sur le deuxième module et vérifie la signature de ce module au moyen de la clé publique associée à la clé privée de l'autorité.

L'ensemble des opérations décrites dans les paragraphes précédents implique l'utilisation de clés sur lesquelles reposent la sécurité de l'application. Ces clés peuvent être cachées dans le module de chargement, stockées dans le lecteur 6, ou bien stockées dans la carte à circuit intégré 31 elle-même. Un autre mode de réalisation possible consiste à implanter le module de déchiffrement et de vérification d'intégrité dans le lecteur 6.

L'objet de l'invention est de s'assurer qu'un pirate ne puisse pas utiliser la carte à circuit intégré d'un utilisateur à son insu, par exemple en modifiant le logiciel filtre pilotant la carte ou le logiciel application, ou bien en implantant un logiciel virus qui court-circuiterait l'application ou le logiciel filtre mis en place. Le mode de réalisation décrit précédemment et ses variantes répondent à ces risques, en permettant la vérification:

- de l'intégrité du logiciel filtre et
- de l'origine et de l'intégrité des commandes envoyées à la carte à travers le lecteur 6, en les authentifiant à l'aide d'un code de type MAC par exemple. La vérification du MAC peut être effectuée par le lecteur 6 ou la carte 31. Une protection équivalente pourrait être obtenue en chiffrant le dialogue entre le logiciel filtre et le lecteur 6. Un logiciel virus cherchant à court-circuiter le logiciel filtre enverrait donc des commandes non authentifiées ou incorrectement chiffrées au lecteur 6 ou à la carte 31 ; en conséquence ces commandes seraient rejetées par le

lecteur ou la carte, empêchant le virus d'arriver à ses fins. Afin qu'un fraudeur ne puisse déterminer les clés utilisées sur un terminal en analysant le fonctionnement d'un autre terminal, les clés utilisées par divers terminaux devront être diversifiées.

Les mécanismes de chiffrement et de signature qui peuvent être envisagés pour répondre au besoin de protection du logiciel filtre sont bien connus des hommes de l'art et reposent sur les techniques cryptographiques existantes exposées, par exemple, dans l'ouvrage de Bruce Schneier intitulé "Applied Cryptography, Protocols, Algorithms, and Source Code in C" publié chez John Wiley and Sons, Inc., 1994, et qui ne seront donc pas décrits en détail ici.

L'implantation du logiciel filtre dans un ordinateur personnel PC ne permet pas de garantir le même degré de sécurité qu'une implantation dans un terminal dédié pouvant offrir des mécanismes de sécurité matériels supplémentaires comme décrit dans les autres formes de réalisation présentées ultérieurement, ces mécanismes procurant une protection physique au logiciel filtre et aux secrets qu'il contient.

Une variante d'exécution du mode de réalisation de la figure 2A est présenté à la figure 2B. Cette variante met à profit la souplesse et la facilité de connexion d'un ordinateur personnel à un réseau. Cette connexion permet en effet le déport d'une partie du logiciel filtre, et en particulier des secrets, dans un serveur sécurisé Ssec.

Dans le cas de la Figure 2B, le logiciel filtre est décomposé en deux modules logiciels, un module F-PC implanté sur l'ordinateur personnel PC 102 et un module F-SE implanté sur un serveur de sécurité Ssec. La mémoire programmable à laquelle il est référence précédemment et stockant le logiciel filtre, est donc dans cette variante d'exécution implantée dans le serveur sécurisé Ssec, c'est-à-dire hors d'atteinte d'utilisateurs non autorisés. De même, le logiciel filtre, ou tout au moins la partie sensible du logiciel filtre F-SE requérant une protection, est exécuté sur le serveur sécurisé Ssec.

Le module logiciel F-PC implanté sur l'ordinateur personnel PC 102 est relié par un canal sécurisé CS au serveur de sécurité Ssec. Ce canal sécurisé est en fait un canal de communication chiffré permettant un échange de données protégé entre les deux modules logiciels filtre F-PC et F-SE et éventuellement une authentification réciproque des deux modules F-PC et F-SE. Ce canal sécurisé peut, par exemple, reposer sur des protocoles de communication bien connus tels que SSL.

L'établissement de ce canal sécurisé CS permet donc au premier module logiciel filtre F-PC de transmettre au deuxième module logiciel filtre F-SE, les requêtes reçues de l'application FAp à travers l'interface logique F-API, ainsi que les informations liées à l'identification de l'application émettant ces requêtes. Ce deuxième module logiciel F-SE va ensuite, après avoir vérifié les informations relatives à l'application et, en fonction de l'application et éventuellement des

droits de l'utilisateur, traduire ces requêtes en une suite de commandes destinées à la carte à puce 31 et au pilotage des échanges de données avec l'utilisateur. Ces commandes crées par le module F-SE sont ensuite envoyées au premier module F-PC qui les aiguille vers l'élément concerné : le PC lui même pour ce qui concerne les commandes de pilotage des échanges avec l'utilisateur ou bien la carte à circuit intégré. Pour que les commandes de pilotage des échanges avec l'utilisateur puissent être exécutées sur le PC, le PC devra comporter un module logiciel I, dit interpréteur. Ce logiciel interpréteur permet l'affichage de messages sur l'écran 4 et la saisie d'information par l'utilisateur sur le clavier 5. Ce module logiciel interpréteur sera plus précisément décrit en regard des figures 4B et 4C.

Ce second mode d'exécution est basé sur les mécanismes décrits à propos du premier mode d'exécution de la figure 2A en ce qui concerne l'identification de l'application (hachage ou signature par exemple) et la protection des commandes envoyées à la carte (ajout d'un code de type authentification de message MAC, par exemple). Il offre par contre un degré de sécurité supérieur dans la mesure où le module logiciel filtre F-SE assurant la traduction des requêtes de haut niveau reçues de l'application Fap est exécuté dans un environnement sécurisé. Dans le contexte de l'invention, le serveur Ssec est dit sécurisé s'il n'est pas accessible physiquement ainsi que logiquement, c'est dire à travers une connexion réseau, à des personnes non autorisées.

Ce second mode d'exécution de la figure 2B est bien adapté à des applications mises en oeuvre dans un environnement fermé ou privatif contrôlé par une autorité centrale, car elle nécessite un serveur protégé dont l'administration doit être centralisée. Ce second mode d'exécution offre de plus la possibilité de définir une politique d'accès centralisée aux services cryptographiques offerts par la carte à circuit intégré. Cette politique d'accès peut être basée sur les applications requérant les services de la carte et sur les utilisateurs eux mêmes. Elle permet, par exemple, dans la cas d'une entreprise ayant distribué à ses employés ou à ses clients des cartes à circuit intégré leur permettant de signer des courriers électroniques ainsi que des transactions bancaires, de s'assurer que seuls les utilisateurs autorisés pourront signer : ce mécanisme peut être mis en oeuvre grâce au canal sécurisé CS. A chaque requête de signature émise par une des applications considérée comme valide par l'entreprise (la messagerie électronique et le logiciel de transactions bancaires), le module logiciel F-SE effectuera une demande d'authentification de l'utilisateur. Cette demande peut, par exemple, être effectuée en envoyant un nombre aléatoire, challenge ou défi via le canal sécurisé CS à la carte 31. Après saisie par l'utilisateur de son code confidentiel, la carte à circuit intégré calculera un mot de passe dynamique en chiffrant le défi à l'aide d'une clé secrète qu'elle contient. Le mot de passe sera ensuite transmis via le canal CS au module logiciel F-SE. Le module logiciel F-SE, connaissant l'utilisateur et donc la clé secrète

contenue dans sa carte, comparera le mot de passe reçu au mot de passe attendu. Ce mécanisme connu sous le nom d'authentification en mode challenge – réponse permet au module logiciel F-SE de valider l'identité de l'utilisateur. Ceci permet donc à l'entreprise ayant remis les cartes à circuit intégré aux utilisateurs de s'assurer que seuls les utilisateurs encore autorisés peuvent par exemple signer des transactions bancaires.

Le serveur Ssec, grâce aux moyens sécurisés et centralisés qu'il représente, permet non seulement une implantation sécurisée du logiciel filtre F-SE mais aussi la possibilité de mettre en place une politique centralisée de contrôle de l'utilisation des services de sécurité offerts par la carte à circuit intégré. Le serveur Ssec permet la mise en place d'une politique centralisée du fait qu'un même serveur peut être en liaison avec une pluralité des modules logiciels F-PC implantés sur les ordinateurs personnels d'une pluralité d'utilisateurs. Le serveur Ssec permet ainsi la définition et le contrôle centralisés des conditions d'utilisation des services de sécurité offerts par les cartes remises aux différents utilisateurs, en fonction du profil de l'application requérant les services et des droits desdits utilisateurs. La mise en place de cette politique centralisée implique donc de stocker dans le serveur les informations nécessaires, c'est-à-dire les droits des utilisateurs d'utiliser tel service de sécurité en liaison avec telle application.

Ce second mode d'exécution de la figure 2B, bien adapté aux environnements privés, est par contre difficilement applicable à des applications ouvertes pour lesquelles la mise en place d'un serveur central sécurisé Ssec n'est pas envisageable.

La Figure 3 illustre un module terminal reprenant des principes d'architecture fonctionnelle similaires à ceux de la Figure 2B dans une forme de réalisation différente, ne nécessitant pas de serveur centralisé. Le module terminal selon la deuxième forme de réalisation de la Figure 3 présente un très haut degré de sécurité, lui permettant ainsi d'assurer directement la protection locale du logiciel filtre F.

Dans le cas de la figure 3, le module terminal 1 se présente sous la forme d'un boîtier, portable ou non, dont une face porte l'écran d'affichage 4 et le clavier 5 et dans lequel sont implantés des circuits électroniques, de préférence de manière telle que ceux-ci soient inaccessibles depuis l'extérieur. Le boîtier 1 contient le lecteur 6 et présente une ouverture de réception de la carte à micro-circuit 31 dans le lecteur 6. Le mode d'exécution décrit en référence aux Figures 3, 4A, 4B et 4C ne doit pas être considéré comme se limitant à un terminal dédié. La description qui suit peut tout à fait être appliquée à un terminal construit autour d'un ordinateur personnel de type PC ou NC.

Selon un premier mode d'exécution, illustré à la figure 4A, de cette deuxième forme de réalisation du module terminal de la figure 3, les circuits électroniques du module terminal 1 sont organisés autour d'un microcontrôleur standard 2 et d'un microprocesseur 3

sécurisé, qui sont connectés entre eux par une liaison et implantés de manière permanente dans le boîtier du module 1. En variante, le microprocesseur 3 peut être enfichable sur le module 1 au moyen d'un connecteur 41 représenté en traits interrompus à la figure 4A. Il est décrit ici un mode d'exécution générique basé sur un microcontrôleur standard. Dans un mode d'exécution particulier qui sera décrit ultérieurement, le microcontrôleur 2 peut en fait être un PC 102 du type de celui présenté dans la Figure 2B.

Le microcontrôleur standard 2 comprend une unité de traitement 2a, de la mémoire temporaire (RAM) 2b, et de la mémoire permanente (ROM) 2c. Il s'agit de préférence d'un microprocesseur "monochip" dont le programme est masqué dans la mémoire permanente 2c et qui intègre dans un même circuit intégré des moyens de gestion ou pilotage d'interfaces standards, l'unité de traitement 2a et les mémoires temporaire 2b et permanente 2c.

Les interfaces ou périphériques gérées par le microcontrôleur 2 comprennent notamment l'écran 4 d'affichage de données, par exemple à cristaux liquides, le clavier 5 pour l'introduction de données par un utilisateur, le lecteur 6 de carte à micro-circuit, une interface 7 de liaison externe, par exemple du type RS 232 ou PCM-CIA, une interface 8 de liaison par infrarouge, et un dispositif DTMF 9 pour la transmission de données sur une ligne téléphonique.

Les composants du module 1 comprennent également une horloge 10 et une source 11 d'alimentation électrique des différents circuits et composants du module 1. La source 11 d'alimentation électrique peut être constituée par des piles ou une batterie si le module 1 est portable et autonome.

La tâche du microcontrôleur standard 2 est de gérer l'environnement, c'est-à-dire de piloter les interfaces 4-9 et l'horloge 10, ainsi que la source d'alimentation 11 pour alimenter sélectivement le microprocesseur sécurisé 3 en énergie électrique dans le cas d'un module 1 autonome.

Le microcontrôleur standard 2 nécessite ainsi peu de puissance de calcul, peu de mémoire temporaire (RAM) et pas de mémoire semi-permanente (EPROM ou EEPROM). Le microcontrôleur 2 est protégé en écriture du fait que ses programmes (pilotage d'interfaces et, comme décrit dans la suite, interpréteur, gestion des horloges et de l'alimentation électrique, etc...) sont masqués en mémoire permanente 2c. Comme cela apparaîtra dans la suite, le microcontrôleur standard 2 peut également contenir un ou plusieurs paramètres secrets, sur la base desquels il peut être authentifié par le microprocesseur sécurisé du module terminal et/ou d'une carte à circuit intégré. Ces secrets doivent donc être protégés en lecture et en écriture. Ils seront de préférence stockés dans la mémoire temporaire (RAM) d'un microprocesseur "mono chip", qui n'est accessible ni en écriture, ni en écriture depuis l'extérieur. Le microcontrôleur standard 2 peut également être pourvu de fonctions de

sécurité complémentaires, par exemple pour interdire des fraudes telles que l'affichage de données différentes de celles provenant du microprocesseur 3.

Il s'agit par conséquent d'un microcontrôleur d'un faible coût et ayant une faible consommation électrique, qui est particulièrement adapté à un produit portable. Ce microcontrôleur peut être par exemple du type MSM 63180 de la Société OKI.

De préférence, deux horloges sont prévues en 10 : une horloge à fréquence basse 10a, par exemple de fréquence 32,368 KHz et une horloge à fréquence élevée 10b, pouvant aller de 1 MHz à 12 MHz par exemple Le microcontrôleur 2 commande la connexion de son horloge système sur l'une ou l'autre de ces deux horloges.

L'horloge lente 10a cadence un dispositif de temporisation 2d du microcontrôleur 2 avec une période de 0,5 s pour réaliser une horloge temps réel dans le module 1. L'unité de traitement 2a peut également fonctionner à l'aide de l'horloge lente 10a pour les fonctions ne nécessitant pas de vitesse de calcul : dans ce cas l'horloge système du microcontrôleur 2 est connectée sur l'horloge lente 10a et l'horloge rapide 10b est arrêtée. Ce mode de fonctionnement permet de limiter la consommation électrique du module 1, ce qui est avantageux si celui-ci est portable et alimenté par une pile électrique.

Le microprocesseur 3 sécurisé en lecture et en écriture comprend une unité centrale 3a et des mémoires temporaire (RAM) 3b et permanente (ROM) 3c, ainsi qu'une mémoire semi-permanente reprogrammable électriquement (EEPROM ou Flash RAM par exemple) 3d pour le stockage, entre autres, des programmes d'application du module 1.

Ce microprocesseur sécurisé 3 est du type de ceux utilisés dans les cartes à micro-circuit et il présente un nombre limité d'entrées et de sortie, ses bus internes étant inaccessibles depuis l'extérieur. De par sa fabrication, il intègre d'autres mécanismes de sécurité propres à ce type de microprocesseur et bien connus des spécialistes de la technique, tels que matrice de sécurité, brouillage de mémoire, contrôle de la fréquence d'horloge, contrôle de la remise à zéro (RESET), etc...

Grâce au fait que le microprocesseur 3 possède une mémoire semi-permanente 3d, il est possible d'y charger depuis l'extérieur, par exemple à partir d'un serveur ou d'une carte à micro-circuit, un ou des programmes d'application. Il est ainsi possible, en fonction des besoins, de faire évoluer la ou les applications (contrôle d'accès, transaction financières et/ou commerciales, porte-monnaie électronique, etc...) auxquelles est destiné le module 1. Il est également possible, si la taille de la mémoire semi-permanente 3d le permet, d'y implanter de nouvelles applications au cours de son utilisation.

Selon la version choisie, le microprocesseur sécurisé 3 peut assurer le calcul de fonctions cryptographiques requérant des calculs importants mis en œuvre dans les

algorithmes asymétriques de type RSA ou DSA, ou bien mettre en œuvre des algorithmes plus simples, par exemple du type DES.

Le microprocesseur sécurisé 3 peut être, par exemple :

- un microprocesseur SIEMENS SLE44C160S, non cryptographique, doté de 14 Ko de mémoire ROM et de 16 Ko de mémoire EEPROM ;

- un microprocesseur SGS THOMSON ST16CF54A cryptographique doté de 16 Ko de mémoire ROM, de 4Ko de mémoire EEPROM et de 480 octets de mémoire RAM ;

- un microprocesseur PHILIPPS P83C858 cryptographique doté de 20 Ko de mémoire ROM et de 8 Ko de mémoire EEPROM.

Le microprocesseur sécurisé 3 est connecté, d'une part par la liaison 12 au microcontrôleur standard 2, d'autre part par des liaisons 13 et 14 à l'interface externe 7 et au lecteur 6 de carte à micro-circuit par l'intermédiaire de commutateurs-adaptateurs d'interface 15 et 16 respectivement. Les commutateurs-adaptateurs 15 et 16 sont commandés par le microcontrôleur standard 2 via des liaisons 17 et 18 respectivement.

Le microcontrôleur standard 2 comprend un programme d'interprétation ou interpréteur 20 (Fig. 4B et 4C) stocké dans la mémoire ROM 2c et permettant à celui-ci d'exécuter des commandes générées par le logiciel de traduction des requêtes de haut niveau faisant partie du ou des programmes d'application, comme cela sera décrit dans la suite. Cet interpréteur 20 permet ainsi au(x) programme(s) d'application stocké(s) dans le microprocesseur sécurisé 3 de piloter les interfaces 4-9 via la liaison 12. Cependant, le ou les programmes d'application peuvent être localisés et exécutés ailleurs que dans le microprocesseur 3 sécurisé en lecture et en écriture, par exemple dans une carte à micro-circuit 31 insérée dans l'interface 6, telle qu'une carte adaptée pour supporter des mécanismes de téléchargement et d'exécution des applications comme décrit dans la norme NF EN 726-3 intitulée "Cartes à circuit intégré et terminaux pour les télécommunications. Partie 3 : Spécifications de la carte indépendantes des applications".

Les programmes d'application peuvent en outre, en fonction des règles de sécurité auxquelles ils sont soumis, être distribués entre ces différentes localisations.

Le schéma fonctionnel de la figure 4B illustre une première configuration d'architecture logicielle du module 1 de la figure 4A dans laquelle l'ensemble des programmes d'application A1, A2, ... An et des fonctions de sécurité (calcul de condensé, algorithmes cryptographiques symétriques tels que DES, triple DES, ou asymétriques tels que proposés par RSA) est mis en œuvre dans le microprocesseur sécurisé 3.

Les applications nommées ci-dessus et dans la suite de la description A1, A2, ... An comprennent au minimum les filtres F1, F2, ..., Fn, et donc en particulier les logiciels de

traduction des requêtes émises par le ou les fournisseurs de services applicatifs FAp faisant partie de l'application principale 54 (Figure 8A).

Le microcontrôleur standard 2 gère l'environnement au moyen de différents programmes de gestion ou gestionnaires d'interface à savoir :

- un gestionnaire 21 du lecteur ou interface 6 de carte à micro-circuit;
- un gestionnaire 22 de l'interface 7 de liaison série ;
- un gestionnaire 23 du clavier 5 ;
- un gestionnaire 24 de l'interface 8 de liaison par infrarouge ;
- un gestionnaire 25 de l'afficheur 4 ;
- un gestionnaire 26 de l'horloge 10 et de la source d'alimentation 11;
- un gestionnaire 27 de l'interface DTMF 9 ;
- un gestionnaire 28 d'autres interface, dans l'hypothèse où le module 1 comporte une ou des interfaces autres que celles représentées à la figure 2.

Ainsi, le microprocesseur sécurisé 3 peut piloter les interfaces au moyen de commandes qui sont interprétées par l'interpréteur 20 et exécutées par le microcontrôleur standard 2 grâce aux gestionnaires 21-28.

La figure 4C illustre une seconde configuration logicielle du module 1 de la figure 4A dans laquelle une ou plusieurs applications Ax et une ou plusieurs fonctions cryptographiques Sx sont stockées dans une mémoire reprogrammable 30a d'un microprocesseur sécurisé 30 d'une carte à micro-circuit 31. Lorsque la carte 31 est introduite dans le lecteur 6, le microprocesseur 30 exécute les applications Ax et les fonctions cryptographiques Sx, tandis que d'autres applications et fonctions de sécurité peuvent être résidentes dans et mises en œuvre par le microprocesseur sécurisé 3 du module 1. C'est ainsi, par exemple, que le microprocesseur 30 de la carte 31 peut assurer une fonction de signature électronique dans l'hypothèse où le microprocesseur sécurisé 3 n'intègre pas un processeur de calcul dédié (cryptoprocesseur). Réciproquement, si le microprocesseur sécurisé 3 intègre un cryptoprocesseur, il est également possible qu'une application présente dans la carte à micro-circuit 31 fasse appel à des commandes cryptographiques du module 1, commandes qui seront exécutées par le microprocesseur sécurisé 3.

Dans cette seconde configuration, qui pour le reste est identique à celle de la figure 4B, l'interpréteur 20 joue vis-à-vis du microprocesseur 30 le même rôle que celui qu'il remplit vis-à-vis du microprocesseur sécurisé 3. Le module 1 peut ainsi exécuter des applications différentes selon le type de carte 31 à micro-circuit introduit dans le lecteur 6, par exemple :

- une authentification de l'utilisateur dans le cadre d'une transaction bancaire (consultation de compte, virement de fonds, etc...) effectuée via une ligne téléphonique au moyen de l'interface DTMF 9 ;

- une consultation du solde d'un porte-monnaie électronique, ou le rechargement de ce porte-monnaie, à partir du module 1, lorsqu'une carte à micro-circuit 31 remplissant la fonction de porte-monnaie est introduite dans le lecteur 6. En outre, le module 1 permet de gérer plusieurs cartes porte-monnaie différentes : porte-monnaie bancaire, porte-monnaie spécifique à une collectivité par exemple ;

- lecture d'un dossier médical sur une carte médicale ;

- lecture de points de fidélité sur une carte dans laquelle des points de fidélité sont attribués à un consommateur en fonction d'achats effectués, de sa participation à des opérations de fidélisation de clientèle, etc...

Le mode d'exécution décrit ci-dessus à la Figure 4A ainsi que les configurations logicielles présentées dans les Figures 4B et 4C s'appliquent, de manière analogue, à un terminal construit autour d'un PC conventionnel équipé en outre du microprocesseur sécurisé 3. Dans ce mode d'exécution, le microcontrôleur 2 correspond au PC 102 tel qu'il est présenté à la Figure 2A, l'unité de traitement 2a correspond au microprocesseur 102c du PC, et les mémoires RAM 2b et permanentes 2c correspondent respectivement à la mémoire RAM 102d et au disque dur 102b. De même les entrées / sorties 102a du PC correspondent aux modules d'interfaces 7, 8 et 12 de la Figure 4A. La connexion entre le microprocesseur sécurisé 3 et le PC 102 peut être une liaison série ou parallèle, ou bien encore une connexion au bus interne du PC, du type PCMCIA, ou une connexion directe sur la carte mère du PC. En variante, le microprocesseur sécurisé 3 peut être intégré de manière fixe, ou amovible via le connecteur 41, au clavier du PC.

Dans ce cas, le module logiciel interpréteur 20 ainsi que les modules logiciels de gestion des périphériques 21 à 28 sont implantés et exécutés sur le PC. L'architecture fonctionnelle de ce mode d'exécution est équivalente à celle présentée à la Figure 2B, le module interpréteur 20 ainsi implanté sur le PC assurant le même rôle que le module interpréteur I de la Figure 2B : il exécute les commandes de pilotage des échanges avec l'utilisateur reçues du logiciel filtre F lui-même implanté de manière sécurisé dans le microprocesseur 3 (Figure 4B) ou la carte à circuit intégré 30 (Figure 4C).

Le schéma de la figure 5 illustre un deuxième mode d'exécution de la deuxième forme de réalisation de l'invention, dans lequel les circuits électroniques du module terminal 1 sont organisés autour d'un seul microcontrôleur 29 remplaçant le microcontrôleur 2 et le microprocesseur 3 et pouvant offrir le même type de protection physique et logique que les

microprocesseurs conçus pour les cartes à circuit intégré. Ce microcontrôleur gère l'ensemble des moyens d'interfaces 4-9 du module terminal. Il comporte une unité de traitement 29a, une mémoire temporaire (RAM) 29b, une mémoire permanente (ROM) 29c et une mémoire semi-permanente (EEPROM) 29d permettant le stockage du logiciel de traduction. L'unité de traitement 29a correspond à la fois à l'unité 2a de traitement de données permettant le pilotage des interfaces et à l'unité 3a de traitement permettant l'exécution du logiciel de traduction. De même que précédemment, le module terminal 1 peut être construit autour d'un ordinateur personnel PC 102 auquel serait connecté au bus interne un microcontrôleur sécurisé 29 pilotant ainsi directement l'écran d'affichage 4 et le clavier 5 du PC.

Dans une variante de réalisation, la mémoire dans laquelle est stockée le logiciel de traduction des requêtes de haut niveau, mémoire volatile de type RAM avec une alimentation de sauvegarde ou semi-permanente (EEPROM ou Flash RAM), peut être externe au microcontrôleur 29. Dans ce cas, le logiciel de traduction peut être chiffré et signé, ou protégé par un code de type MAC ("Message Authentication Code") de manière à assurer à la fois son intégrité et sa confidentialité. Le logiciel est lu par le microcontrôleur 29, déchiffré puis exécuté.

Selon un troisième mode d'exécution, représenté à la figure 6, de la deuxième forme de réalisation de l'invention, le module terminal 101 est dépourvu de microprocesseur sécurisé 3. Sur cette figure 6, les mêmes numéros de référence qu'à la figure 4A ont été conservés pour désigner les mêmes éléments. Le microcontrôleur 2 pilote l'interface 6 et le commutateur-adaptateur 15 pour permettre la connexion du microprocesseur sécurisé 130 d'une carte à micro-circuit programmable 131 présente dans l'interface 6 avec l'interface de liaison externe 7. Dans ce cas, l'ensemble des applications A et des fonctions cryptographiques C sont mémorisées dans une mémoire semi-permanente 130a (EEPROM ou Flash RAM) du microprocesseur sécurisé 130 de la carte à micro-circuit programmable 131, et mises en œuvre par ce dernier comme décrit à la figure 4C à propos des applications Ax et des fonctions cryptographiques Cx.

Dans les exemples décrits précédemment, dans un but de simplification, le microprocesseur 30, 130 de la carte à circuit intégré ainsi que le microprocesseur sécurisé 3 éventuellement implanté dans le module terminal comporte un seul port de communication. Ceci implique que dans ces exemples, les échanges entre les différentes entités, à savoir l'unité électronique 154 (figure 8) contenant l'application principale, le microprocesseur sécurisé 3 et le microprocesseur 30, 130 de la carte circuit intégré se font à travers le microcontrôleur 2 ou 29 du module terminal. Ces descriptions ne doivent pas être considérées comme limitatives : d'autres mises en œuvre peuvent être envisagées dans le cadre de la présente invention. En effet, les microprocesseurs sécurisés de carte à circuit intégré actuellement disponibles,

utilisables pour la carte elle même (microprocesseur 30, 130) ou dans le module terminal (microprocesseur 3), peuvent comporter deux ports de communication. Différentes formes de réalisation optimisant les flux de communication sont donc aisément envisageables avec ce type de microprocesseur. Dans le cas de la figure 4C, par exemple, un des ports de la carte à circuit intégré 31 peut être dédié au pilotage de l'interface utilisateur et donc relié au microcontrôleur 2, l'autre port étant relié à l'unité électronique comportant l'application principale moyennant une adaptation d'interface appropriée.

Suivant une caractéristique importante de l'invention, un logiciel filtre est implanté dans la mémoire reprogrammable EEPROM associée au microprocesseur sécurisé 3 ou 29 du module terminal 1 et/ou au microprocesseur sécurisé 30, 130 de la carte 31, 131. Ce logiciel filtre traduit de manière connue les requêtes de haut niveau en provenance du serveur Sap ou de l'ordinateur personnel PC en séquences de commandes élémentaires exécutables par ces microprocesseurs (commandes qui sont notamment définies par la partie 4 de la norme ISO 7816-4). En outre, suivant l'invention, ce logiciel filtre traduit ces requêtes de haut niveau en séquences d'échanges de données entre le module terminal 1, 101 et un utilisateur via les moyens d'interface tels que l'afficheur 4 et le clavier 5.

Cette solution offre l'avantage de réduire considérablement le débit de données échangé entre le module terminal 1, 101 et le serveur Sap ou le PC, mais requiert une implantation sécurisée du logiciel de traduction pour empêcher que les instructions envoyées à la carte à micro-circuit soient modifiées.

Ce logiciel filtre fait partie intégrante de la partie du logiciel d'application implantée dans le module terminal 1 et/ou la carte 31, 131 et il est donc téléchargeable.

La figure 7 illustre l'architecture logicielle conventionnelle d'une carte à micro-circuit ("smart card").

Les différentes couches de logiciels sont représentées par un bloc 43 qui comprend une couche logicielle 44 "protocole de communication" permettant de recevoir des commandes. Ces commandes sont décodées par une couche logicielle 45 "Interprétation commandes APDU" (APDU : "Application Protocol Data Unit" dont le rôle est d'orienter les commandes vers des modules de traitement qui peuvent être :

- un logiciel 46 de services de gestion de fichiers sécurisés ;
- un logiciel 47 de services cryptographiques ;
- un ou d'autres logiciels d'application 48

Les modules de traitement 46, 47, 48 s'appuient sur des services de base offerts par le système d'exploitation 49 de la carte à micro-circuit.

La figure 8A illustre l'architecture logicielle d'un système de mise en œuvre de transactions sécurisées faisant appel à des modules terminaux 1 dotés d'un microprocesseur sécurisé 3, conformément au mode d'exécution de l'invention de la figure 4A.

Le bloc 51 désigne les logiciels exécutés par le microprocesseur sécurisé 3 du module terminal 1, le bloc 52 les logiciels exécutés par le microcontrôleur 2 ou PC 102 du module terminal 1, le bloc 53 les logiciels exécutés par le microprocesseur 30 d'une carte à micro-circuit 31, et le bloc 54 le logiciel principal d'application, ou Fournisseur de services applicatifs, implanté dans le serveur Sap ou un ordinateur personnel PC.

Le bloc 51 est similaire au bloc 43 de la figure 7, c'est-à-dire que le microprocesseur sécurisé 3 a une architecture semblable à celle d'une carte à circuit intégré. Le bloc 51 comprend:

- un logiciel 60 de protocole de communication.
- un système d'exploitation 61
- un bloc 62 représentant la partie du logiciel d'application implantée dans le module terminal 1, cette partie du logiciel d'application étant essentiellement constituée du logiciel filtre précité. Différents modules logiciels de ce type correspondant à différentes applications peuvent cohabiter dans le microprocesseur sécurisé 3.
- optionnellement, un logiciel 63 permettant d'assurer l'authentification du microcontrôleur standard 2 par le microprocesseur sécurisé 3 et l'authentification du microprocesseur sécurisé 3 du module terminal 1 par le microprocesseur 30 de la carte 31,
- un logiciel 64 de gestion de fichier sécurisé,
- un logiciel 65 de services cryptographiques.

Le bloc 52 comprend :

- un logiciel 70 de protocole de communication ;
- un interpréteur de commandes 71 correspondant au logiciel 20 des figures 4B et 4C ;
- un logiciel d'authentification 72 permettant, en liaison avec le logiciel 63, l'authentification du microcontrôleur standard 2 par le microprocesseur sécurisé 3 du module terminal 1 ;
- des logiciels 73 de gestion des ressources internes du microcontrôleur 2 ;
- des logiciels 74 de pilotage des interfaces avec l'utilisateur (gestionnaires 23 et 25 de l'écran 4 et du clavier 5) ;
- des logiciels 75 de pilotage des interfaces de communication 7, 8 et 9 (gestionnaires 22, 24, 27) ;

Enfin, le bloc 53 est similaire au bloc 43, mais ne comporte pas, dans l'exemple décrit par la figure 8A, de logiciel d'application ou filtre. Il comprend :

- un logiciel 80 de protocole de communication,
- un logiciel 81 d'interprétation de commandes APDU,

- un logiciel 82 de services de gestion de fichier sécurisé (contrôle du PIN par exemple),

- un logiciel 83 de services cryptographiques (calculs cryptographiques symétriques à clés secrètes ou asymétriques, à clés publiques et clés privées, etc...) permettant, entre autres, d'assurer, en liaison avec le logiciel 63, l'authentification du microprocesseur sécurisé 3 du module terminal 1 par le microprocesseur 30 de la carte 31,

- le système d'exploitation 84 du microprocesseur 30 de la carte 31.

Le protocole de communication 60, 70, 80 permet de gérer les échanges de données entre:

- le microprocesseur 30 de la carte 31 et le microcontrôleur standard 2 ou PC 102 du module terminal 1 ;

- le microprocesseur sécurisé 3 et le microcontrôleur 2 du module terminal 1 ;

- le microprocesseur sécurisé 3 du module terminal 1 et le microprocesseur 30 de la carte 31.

La figure 8B est une vue similaire à la figure 8A illustrant l'architecture logicielle du système dans le cas où le module terminal 101 ne comporte pas le microprocesseur sécurisé 3, conformément au troisième mode d'exécution du deuxième mode de réalisation de l'invention de la figure 6.

Sur la figure 8B, le bloc 152 désigne les logiciels exécutés par le microcontrôleur 2 du module terminal 101, le bloc 153 les logiciels exécutés par le microprocesseur 130 d'une carte à micro-circuit programmable 131, et le bloc 154 le logiciel principal d'application implanté dans le serveur Sap ou un ordinateur personnel PC.

Le bloc 152 comprend les mêmes logiciels 70, 71 et 73 à 75 que le bloc 52 de la figure 8A, et un bloc 76 qui est un logiciel d'authentification du microcontrôleur standard 2 du module terminal 101 vis-à-vis du microprocesseur 130 de la carte 131.

Le bloc 153 relatif au microprocesseur 130 de la carte 131 comprend les logiciels 62 et 80 à 84 des blocs 51 et 53 de la figure 8A, ainsi qu'un logiciel 77 permettant, en liaison avec le logiciel 76, d'assurer l'authentification du microcontrôleur standard 2 du module terminal 101 vis-à-vis du microprocesseur 130 de la carte 131.

A la différence d'un système conventionnel, dans le système de transaction sécurisée selon l'invention, le logiciel filtre 62 qui traduit les requêtes de haut niveau de l'application en commandes élémentaires exécutables par une carte à micro-circuit est implanté dans l'environnement utilisateur sécurisé, c'est-à-dire soit dans le module terminal 1 (pour les applications A1, A2.....An des modes d'exécution des figures 4A-4C et 5), soit dans une carte 31, 131 à mémoire semi-permanente utilisable avec le module terminal 1, 101 (pour les applications Ax du mode de réalisation de la figure 4C et pour toutes les applications du mode de réalisation de la figure 6).

Outre sa fonction de gestion d'une carte à micro-circuit, ce logiciel filtre 62 gère les interactions avec l'utilisateur, c'est-à-dire les séquences d'échange de données entre un utilisateur et le module terminal qui sont requises dans le cadre d'une application, échanges qui ont lieu par l'intermédiaire des moyens d'interface, à savoir l'écran 4 et le clavier 5. Il est à noter que l'invention n'est pas limitée à l'utilisation d'un écran et d'un clavier comme interfaces avec l'utilisateur et que tout autre type d'interface, par exemple vocale, présentant l'ergonomie requise, pourrait convenir.

Grâce à l'implantation sécurisée du logiciel filtre 62 dans le microprocesseur sécurisé 3 ou 29 du module terminal 1 ou le microprocesseur 30, 130 de la carte à micro-circuit 31, 131, la sécurité des transactions est assurée. En effet, les clés et règles nécessaires pour accéder à des fichiers de la carte à micro-circuit 31, 131 sont contenues dans le logiciel de traduction 62 et sont donc inaccessibles à des tiers.

Les fonctions remplies par le logiciel filtre 62 seront illustrées ci-après en prenant l'exemple d'une application visant le commerce électronique. L'application met en œuvre les entités suivantes :

- un acheteur
- un commerçant,
- une banque.

Le commerçant dispose d'un serveur de commerce électronique Sap (serveur Web) accessible depuis le réseau Internet. Les acheteurs sont équipés de:

- un ordinateur PC permettant d'accéder au serveur Sap de commerce électronique, et grâce auquel l'acheteur peut consulter un catalogue de marchandises.
- une carte à circuit intégré 31 délivrée par la banque et dont le microprocesseur 30 contient une clé privée, mais ne dispose pas de capacités cryptographiques permettant d'effectuer une signature,
- un module terminal 1 selon le mode de réalisation de la figure 4A, doté d'un microcontrôleur standard 2, d'un microprocesseur sécurisé 3 disposant de capacités cryptographiques permettant la signature d'un message, d'un clavier 5, d'un afficheur 4, d'une interface carte à circuit intégré 6 et d'une interface série 7 pour sa connexion à un ordinateur PC.

Les principes de fonctionnement sont les suivants : la transaction est signée par le module terminal 1 à l'aide d'une clé privée détenue par la carte 31. Cette clé privée est protégée par un code porteur confidentiel (PIN) que l'acheteur doit saisir en milieu sécurisé, donc sur le terminal 1, et par une authentification préalable du terminal 1 par la carte 31 à l'aide d'une clé secrète Kauth. De plus la clé privée est transmise de manière chiffrée (par une

clé Kchif) de manière à établir un canal de communication sécurisé entre le microprocesseur 30 de la carte à circuit intégrée 31 et le microprocesseur sécurisé 3 du terminal 1.

La figure 9 illustre les échanges entre les différentes entités :

a. l'acheteur constitue sa commande sur l'ordinateur PC,

b. l'ordinateur PC élabore la transaction à faire signer par l'acheteur (référence article, prix) et demande la signature de cette transaction au module terminal 1,

c. le module terminal vérifie l'origine de la demande de signature puis sollicite la saisie du code PIN par affichage d'un message "saisie PIN" sur son afficheur 4,

d. l'acheteur saisit son code porteur (code PIN) sur le clavier 5 du module terminal 1,

e. le PIN est envoyé par le module terminal 1 à la carte 31 pour vérification. Cette vérification étant positive, elle provoque la levée d'une de deux conditions d'accès à la lecture de la clé privée,

f. le module terminal 1 affiche la transaction sur son afficheur 4,

g. l'acheteur donne son accord, par appui sur une touche "validation" du clavier 5 du module terminal 1,

h. le module terminal 1 soumet une demande d'authentification externe à la carte 31. Cette authentification externe permet au microprocesseur sécurisé 3 du module terminal 1 de s'authentifier vis-à-vis du microprocesseur 30 de la carte 31 et de lever ainsi la deuxième protection d'accès à la clé privée. Cette authentification se fait en mode challenge/réponse sur la base d'un secret., Kauth, partagé par le module terminal 1 et la carte 31,

i. le module terminal 1 envoie une demande de lecture de clé privée à la carte 31,

j. toutes les conditions d'accès étant remplies, la carte 31 accepte la demande de lecture, et renvoie la clé privée, chiffrée par une clé secrète, Kchif, partagée par la carte 31 et le module terminal 1,

k. le module terminal 1 déchiffre la clé privée, signe la transaction au moyen de la clé privée, détruit la clé privée, se déconnecte de la carte 31 et envoie e la transaction signée à l'ordinateur PC qui la transmet au serveur S.

Cet exemple peut être transposé aisément à une transaction électronique effectuée sans ordinateur PC, le module terminal 1 se connectant directement à un serveur Sap par une liaison modem (figure 3), l'acheteur entrant la commande (référence produit) sur le module terminal 1.

Il est à noter que l'authentification du microprocesseur sécurisé 3 par la carte peut aussi être effectué à travers la commande de lecture de clé privée en lui associant un code d'authentification MAC (Message Authentification Code) calculé au moyen d'une clé secrète.

Cet exemple montre que le logiciel filtre 62 permet de traduire une requête de haut niveau "demande de signature de transaction" en une multitude de requêtes élémentaires adressées aux différentes interfaces du module terminal 1, à savoir l'interface 6 avec la carte à circuit intégré 31, l'interface afficheur 4, l'interface clavier 5, l'interface de connexion à l'ordinateur PC ou au serveur Sap.

Un tel logiciel filtre de traduction a un rôle d'écran, de filtre entre le monde extérieur, c'est à dire les applications, et les périphériques qu'il gère.

Il améliore la sécurité offerte du fait que :

1. il impose un séquencement aux ordres élémentaires envoyés. Par exemple, dans le cas illustré ci-dessus, il impose que la transaction soit validée par l'utilisateur avant d'être signée.

2. il dispose seul des paramètres secrets permettant de générer et d'authentifier ces ordres élémentaires. Ainsi il dispose seul des clés d'authentification et de chiffrement permettant de lire et déchiffrer la clé privée.

Lorsque le logiciel filtre est exécuté dans le microprocesseur sécurisé 3 du module terminal 1, ces propriétés permettent d'imposer une politique d'accès à la carte 31, politique qui n'est pas toujours complètement imposée par la carte elle-même, ou d'étendre les capacités d'une carte (capacité de signature déléguée au module terminal, utilisation dans un contexte non prévu lors de son déploiement initial).

Les avantages offerts en terme de sécurité par l'exécution du logiciel filtre dans le microprocesseur sécurisé du module terminal ou dans celui de la carte à circuit intégré ne sont possibles que parce que le logiciel s'exécute dans un environnement sécurisé permettant d'assurer que :

- les secrets contenus par le logiciel filtre ne sont pas accessibles du fait qu'ils sont mémorisés au sein du microprocesseur sécurisé 3, 29, 30 ou 130,
- la confidentialité et l'intégrité du logiciel filtre sont préservés, du fait que ce logiciel est mémorisé dans la microprocesseur sécurisé 3, 29, 30 ou 130.

Dans le cas où le module terminal 1 est un produit dédié, disposant de ses propres interfaces, afficheur 4 et clavier 5, l'objectif de sécurité est atteint grâce au fait que le logiciel pilotant les échanges de données avec l'utilisateur ne peut être modifié, dans la mesure où il est stocké de manière définitive dans la mémoire permanente 2c du microcontrôleur 2 ou de manière sécurisée dans le microcontrôleur 29. L'utilisateur peut ainsi valider en toute confiance le contenu de sa transaction grâce à l'afficheur 4 et au clavier 5, rendant optionnel la nécessité de vérifier l'identité de l'application ou l'origine et l'intégrité des requêtes.

D'autres mécanismes peuvent encore améliorer le niveau de sécurité de la chaîne de confiance entre le microprocesseur sécurisé de la carte à circuit intégré, l'éventuel

microprocesseur sécurisé du module terminal, le microcontrôleur standard ou le PC du module terminal et l'utilisateur. Ces mécanismes sont les suivants :

A) téléchargement sécurisé du logiciel filtre ;

B) authentification du microcontrôleur standard par le microprocesseur sécurisé ou, ce qui est équivalent mais mieux adapté dans le cas d'un mode d'exécution du terminal autour d'un PC, authentification du module logiciel interpréteur I (20) par le logiciel filtre F (62), et/ou établissement d'un canal de communication sécurisée entre ces deux microprocesseurs ou les logiciels I et F,

C) protection d'un secret par le microcontrôleur standard ,

D) authentification mutuelle et établissement d'un canal de communication sécurisé entre le microprocesseur sécurisé de la carte à circuit intégré et le microprocesseur sécurisé du module terminal,

E) authentification du module terminal, et éventuellement du couple module terminal-carte,

F) authentification de la carte à micro-circuit par le module terminal.

A) **Téléchargement sécurisé du logiciel filtre**

L'organigramme de la figure 10 illustre le processus de téléchargement d'un programme d'application (logiciel filtre) dans le microprocesseur sécurisé 3 ou 29 du module 1 ou le microprocesseur sécurisé 30, 130, d'une carte 31, 131 présente dans le lecteur 6. Ce téléchargement peut être effectué à partir d'un serveur Sap via, par exemple, l'ordinateur personnel PC et l'interface 7 de liaison externe ou l'interface 8 de liaison infrarouge, ou directement au moyen d'une liaison téléphonique grâce à l'interface 9 de liaison par DTMF. Le téléchargement peut également être effectué dans le microprocesseur sécurisé 3 ou 29 (si le module terminal en est équipé) à partir d'une carte à micro-circuit introduite dans le lecteur 6.

A l'étape 32, la zone de la mémoire 3d allouée au programme d'application à recevoir est vide et le microprocesseur 3 est en attente du chargement du programme d'application à la suite d'une requête de chargement.

L'étape suivante 33 correspond à une procédure d'authentification par le microprocesseur 3 de l'entité appelée à télécharger le programme d'application (Emetteur). Cette procédure d'authentification peut faire appel, par exemple, à des mécanismes de chiffrement bien connus des spécialistes de la technique, par exemple des mécanismes symétriques à clés secrètes partagées ou des mécanismes asymétriques à clé privée et clé publique.

L'étape 34 est un test visant à déterminer si la procédure d'authentification a réussi : dans la négative, le message "accès refusé" est affiché sur l'écran 4 (étape 42) et le programme retourne à l'étape 32; dans l'affirmative, le processus de chargement du programme d'application commence à l'étape 35.

L'étape 36 correspond au stockage dans la mémoire EEPROM 3d des trames de données transmises par l'entité assurant le téléchargement.

L'étape 37 est un test pour déterminer si le téléchargement est achevé : dans la négative, le programme de téléchargement revient à l'étape 36 et le téléchargement se poursuit ; dans l'affirmative, il est procédé à l'étape 38 à une vérification de l'intégrité des données reçues par le microprocesseur 3. A cet effet, un code d'authentification de message (MAC) peut être associé au programme téléchargé pour permettre de vérifier non seulement son intégrité, mais également son origine. Le MAC peut être produit en utilisant un mécanisme de cryptographie symétrique (DES en mode chaîné CBC). La vérification de l'origine et de l'intégrité peut aussi être réalisée à l'aide d'un mécanisme de cryptographie asymétrique : un condensé du logiciel téléchargé est signé par l'émetteur à l'aide de sa clé privée ; le microprocesseur sécurisé 3 vérifie ensuite la signature à l'aide de la clé publique de l'émetteur.

Il est à noter que dans ce dernier exemple, la clé publique par principe ne nécessite pas de rester confidentielle. Cependant la sécurité apportée par le microprocesseur assure l'intégrité du logiciel, empêchant un fraudeur de modifier le logiciel pour supprimer la vérification de signature ou simplement de substituer à la clé publique initialement prévue une clé publique pour laquelle il connaîtrait la clé privée associée.

Si d'après le test 39, il s'avère que les données reçues sont correctes, un drapeau indiquant que le programme d'application reçu est validé est élaboré à l'étape 40. Dans le cas contraire, le programme de téléchargement revient à l'étape 32 de départ.

Ce processus de chargement du logiciel d'application, donc du logiciel filtre, dans la mémoire reprogrammable sécurisée (3d, 30a, 130a suivant le mode de réalisation), comporte des mécanismes permettant de confirmer l'origine et l'intégrité des données reçues de l'émetteur du logiciel. Ceci permet d'interdire le téléchargement par un fraudeur d'un logiciel filtre qui serait susceptible de mettre en œuvre des transactions dans le module terminal 1, 101 à l'insu de l'utilisateur.

B) Authentification du module logiciel interpréteur I, 20, 71 par le logiciel filtre F, 62 ou, ce qui est équivalent dans le mode d'exécution correspondant, authentification du microcontrôleur standard 2 par le microprocesseur sécurisé, et/ou établissement d'un canal de communication sécurisé entre ces deux logiciels ou ces deux microprocesseurs.

Pour qu'un utilisateur puisse avoir une totale confiance dans le module terminal au moyen duquel il effectue des transactions, il est nécessaire :

- d'authentifier les données transmises du logiciel interpréteur 20, 71 au microprocesseur sécurisé 3, 30 ou 130 exécutant le logiciel filtre ;
- d'assurer que les données transmises par le logiciel filtre pour être affichées par l'intermédiaire du logiciel interpréteur du module terminal 1, 101 possédé par l'utilisateur ne peuvent l'être que par celui-ci.

Lorsque les moyens de pilotage des échanges de données avec l'utilisateur, c'est à dire le logiciel interpréteur 20, 71, sont implantés de manière fixe et non modifiable dans le module terminal 1, 101, comme par exemple dans la mémoire ROM 2c du microcontrôleur standard 2, l'authentification du module logiciel est équivalente à l'authentification du microcontrôleur.

De même, lorsque le logiciel filtre est implanté de manière à ne pas pouvoir être modifié par une personne non autorisée, dans des moyens de traitement sécurisés tels que le microprocesseur sécurisé 3, la carte à circuit intégré ou bien le serveur sécurisé Ssec, une authentification effectuée par ces moyens sécurisés est équivalente à une authentification effectué par le logiciel filtre lui-même.

Dans la description qui suit, nous décrirons les mécanismes d'authentification des moyens logiciels de pilotage des interfaces ou logiciel interpréteur 20, 71 par le logiciel filtre.

Différentes solutions permettent de remplir ces conditions.

Une première solution consiste à chiffrer toutes les données échangées entre le le logiciel interpréteur 20, 71 et le logiciel filtre.

Une deuxième solution consiste à faire procéder à l'authentification du logiciel interpréteur 20, 71 par le le logiciel filtre et/ou à établir un canal de communication sécurisé entre ces deux logiciels.

Ces deux solutions impliquent nécessairement qu'au moins un paramètre secret connu du logiciel filtre F, 62, soit stocké dans le logiciel interpréteur 20, 71.

Selon la deuxième solution, le logiciel filtre F, 62 authentifie le logiciel interpréteur 20, 71, selon un processus conventionnel d'authentification, sur la base d'une information transmise par le logiciel interpréteur 20, 71, et combinée avec le paramètre secret. Au niveau du logiciel interpréteur 20, 71, cette procédure d'authentification est mise en œuvre par le logiciel 72 (figure 8A) ou le logiciel 76 (figure 8B), suivant la forme de réalisation du module terminal.

Ce mécanisme d'authentification peut également s'appliquer aux messages échangés entre les deux logiciels pour construire des codes d'authentification des messages permettant de garantir l'origine et l'intégrité de chaque message transmis.

Dans le cas du mode d'exécution décrit à la Figure 4A, cette solution requiert cependant que, de préférence, une protection physique de la liaison entre les deux microprocesseurs soit assurée pour interdire à un fraudeur de lire les données échangées, et en particulier le code d'identification personnel (PIN) de la carte que l'utilisateur peut être amené à introduire via le clavier 5 pour la mise en oeuvre des transactions.

C) **Protection d'un paramètre secret par le microcontrôleur standard 2**

La description précédente montre la nécessité de stocker au moins un paramètre secret dans le logiciel interpréteur. Le mode d'exécution du terminal à partir d'un PC, dans lequel le logiciel interpréteur est exécuté sur le PC lui-même, offre donc de par la sécurité limitée du PC un degré de sécurité limité bien que suffisant pour empêcher un virus de se substituer au logiciel interpréteur. Un degré de sécurité supérieur est obtenu en implantant le logiciel interpréteur dans la ROM 2c du microcontrôleur standard 2. Pour améliorer la sécurité, le paramètre secret du microcontrôleur 2 pourra être stocké dans la mémoire temporaire, et cela à la fabrication du produit ou, éventuellement, lors de l'insertion du microprocesseur sécurisé 3 s'il est amovible, ou d'une carte à circuit intégré. Cette opération a pour but d'établir une confiance entre les deux microprocesseurs. Toute précaution utile doit être prise lors de cette opération pour s'assurer de l'authenticité du microcontrôleur 2 (opération effectuée en usine, opération protégée par des clés dites de transport elles-mêmes stockées dans la mémoire temporaire du microcontrôleur 2 en usine, et dont la connaissance conditionne l'opération d'initialisation dudit paramètre secret). En outre des mécanismes conventionnels de détection d'intrusion (contacts...) seront mis en place, pour provoquer l'effacement de la mémoire temporaire en cas d'intrusion (coupure alimentation...).

D) **Authentification mutuelle et établissement d'un canal de communication sécurisé entre le microprocesseur de la carte à circuit intégré et le microprocesseur sécurisé du module terminal**

Cette authentification mutuelle et l'établissement du canal de communication sécurisée sont réalisés par la mise en œuvre de mécanismes identiques à ceux utilisés entre le microcontrôleur standard 2 et le microprocesseur sécurisé exécutant le logiciel filtre comme décrit au point B) ci-dessus.

E) **Authentification du module terminal**

Il est important de se prémunir vis-à-vis de toute attaque contre l'ensemble clavier 5, afficheur 4, microprocesseur sécurisé 3, visant par exemple à effectuer des contrefaçons de

module terminal , à substituer un module terminal par un module terminal contrefait dans le but de récupérer des informations saisies par l'utilisateur (espionnage clavier), d'accéder aux secrets d'une carte à circuit intégré, d'effectuer des fausses signatures.

Pour cela, il pourra être ajouté un mécanisme permettant à l'utilisateur d'authentifier son terminal.

Cet objectif est atteint grâce à un processus de personnalisation automatique.

Authentification du module terminal seul

La personnalisation peut consister en le calcul d'un mot de passe facile à se rappeler généré et affiché par le terminal en fonction des paramètres secrets contenus par le ou les microprocesseurs du terminal, lorsque l'utilisateur introduit un PIN. Si le terminal comporte par exemple deux microprocesseurs, le mot de passe est stocké dans le microprocesseur sécurisé, chiffré par le PIN et une clé secrète X, puis transmis au microcontrôleur 2 pour déchiffrement avec la clé X stockée également dans le microcontrôleur 2 et le PIN introduit par l'utilisateur. Ce mécanisme vise a se prémunir contre la substitution de l'un des deux microprocesseurs.

Le même principe peut être appliqué à un couple carte/terminal à chaque fois qu'une carte à micro-circuit est utilisée avec le module terminal. La personnalisation peut consister par exemple en le calcul, au moyen du logiciel de traduction, d'un mot de passe basé sur une information secrète contenue dans le microprocesseur sécurisé de la carte et d'une ou plusieurs informations secrètes contenues dans module terminal. Le même principe que celui décrit ci-dessus peut être utilisé pour calculer le mot de passe. Ce mot de passe, généré lors de la première utilisation du module terminal en conjonction avec la carte et connu de l'utilisateur, est affiché sur l'écran 4 lors des utilisations subséquentes du module terminal avec la carte. L'utilisateur peut ainsi le vérifier et avoir ainsi l'assurance que le terminal en sa possession, constitué du module terminal couplé à la carte, est bien authentique.

F) **Authentification de la carte à micro-circuit par le module terminal**

Pour accroître encore la sécurité du système de transaction suivant l'invention, un processus conventionnel d'authentification peut être mis en œuvre afin d'assurer l'authentification par le module terminal 1, 101 de la carte à micro-circuit utilisée. Un tel processus d'authentification permet notamment d'éviter que le numéro d'identification personnel (PIN) de l'utilisateur, que celui-ci introduit dans le module 1, 101 par le clavier 5 pour exécuter une transaction sécurisée, soit capturé par une carte falsifiée qui aurait été substituée par un fraudeur à la carte authentique de l'utilisateur puis que ce fraudeur récupérerait pour lire le PIN sur la carte falsifiée. L'authentification peut, par exemple, être effectuée par un mécanisme classique de type défi / réponse au moyen d'un secret partagé

entre la carte et le module terminal en utilisant une cryptographie symétrique ou bien, comme cela a déjà été décrit précédemment, au moyen d'une clé privée stockée par la carte permettant le chiffrement du défi ou challenge à l'aide d'un algorithme asymétrique, le module terminal vérifiant la réponse à l'aide de sa clé publique.

L'architecture du système de transaction ainsi que les mécanismes de sécurisation décrits ci-dessus confèrent une très grande sécurité aux transactions effectuées au moyen du module terminal 1, 101.

Ce module terminal permet :

- grâce au clavier 5, à l'écran 4 et à la protection des données échangées avec l'utilisateur, d'étendre la nature des services réellement sécurisés que peut fournir une carte à micro-circuit ;

- d'utiliser la carte dans le contexte d'un environnement non sécurisé (ordinateur personnel PC susceptible d'être affecté par des virus ou programmes pirates), en l'isolant hermétiquement de cet environnement grâce à une architecture logicielle et/ou matérielle qui contrôle strictement l'accès à la carte, c'est à dire qui contrôle les commandes envoyées aux fonctions cryptographiques contenues dans la carte.

Le module terminal peut revêtir différentes formes telles que :

- un lecteur de carte à circuit intégré, connectable à un ordinateur via différentes interfaces (PCMCIA...) ou non (connexion à un serveur via modem uniquement) ;
- un ordinateur (PC) dont les interfaces utilisateur sont constituées par l'écran et le clavier du PC, et qui comporte un lecteur de carte à circuit intégré. Ce PC inclura des moyens logiciels et / ou matériels (tels qu'un second microprocesseur sécurisé, le microcontrôleur standard étant constitué par le PC) pour assurer l'intégrité et la confidentialité du logiciel filtre. Par ordinateur on entend un ordinateur de type PC, mais également un PDA (" Personal Digital Assistant " ou Assistant Numérique Personnel) ;
- un clavier, éventuellement muni d'un écran d'affichage LCD, dans lequel est intégré un microprocesseur sécurisé et une interface carte à circuit intégré ;
- un téléphone muni éventuellement d'un afficheur, dans lequel est intégré un microprocesseur sécurisé et une interface carte à circuit intégré ;
- un décodeur (set-top box) de réseau câblé de TV intégrant un lecteur ce carte à circuit intégré connecté à un poste de télévision, le poste de télévision, un clavier ou éventuellement la télécommande associé au décodeur ou à la télévision servant de moyens d'interface avec l'utilisateur ;
- plus généralement tout équipement sécurisable par l'intégration d'un microprocesseur sécurisé dans lequel pourra être installée une application dite sensible,

ou par l'intégration d'une interface carte à circuit intégré permettant le pilotage dudit équipement par une application déportée dans une carte à circuit intégré.

L'ensemble de la description précédente décrit un terminal destiné à être utilisé avec une carte à circuit intégré ou "smart card". La carte à laquelle il est fait référence est en fait un outil permettant la mise en oeuvre de fonctions cryptographiques et personnalisé par rapport à un utilisateur au moyen d'au moins un secret. Il est évident que l'objet de l'invention ne se limite pas à un outil de forme donnée tel que celui de la carte à circuit intégré. L'invention couvre aussi la mise en oeuvre de dispositifs personnels de sécurité pouvant offrir des fonctions équivalentes à celle d'une carte à circuit intégré, mais présentés sous une forme différente, tels que les produits " iButton ", " Java Ring " ou jeton (" token ").

REVENDICATIONS

1. Terminal pour la mise en œuvre, par un utilisateur, de transactions électroniques sécurisées en liaison avec au moins une application implantée sur une unité électronique, ledit terminal comprenant :

- un module terminal comportant au moins :

* des premiers moyens d'interface avec ladite application pour en recevoir des requêtes relatives auxdites transactions,

* des deuxièmes moyens d'interface avec ledit utilisateur,

* des troisièmes moyens d'interface avec un dispositif personnel de sécurité,

* des premiers moyens de traitement de données comprenant au moins des premiers moyens logiciels de pilotage desdits moyens d'interface, et

- un dispositif personnel de sécurité comportant au moins des deuxièmes moyens de traitement de données sécurisés comprenant au moins des deuxièmes moyens logiciels d'exécution de commandes élémentaires et des moyens d'exécution de calculs cryptographiques,

caractérisé en ce que :

- ledit terminal (1, 31 ; 101, 131) est adapté pour recevoir lesdites requêtes de ladite application (Fap) implantée sur la dite unité électronique (Sap ; PC) sous la forme de requêtes de haut niveau indépendantes dudit dispositif personnel de sécurité,

- l'un au moins dudit module terminal (1; 101) et dudit dispositif personnel de sécurité comprend :

* au moins une mémoire reprogrammable (3d ; 30a ; 102b ; 130a ; Ssec) de stockage d'au moins un logiciel filtre (F, 62), traduisant lesdites requêtes de haut niveau en au moins l'une de :

(i) au moins une commande élémentaire ou une séquence de commandes élémentaires exécutables par lesdits deuxièmes moyens logiciels (80-84) desdits deuxièmes moyens de traitement de données (30 ; 130), ou

(ii) au moins une séquence d'échange de données entre ledit module terminal (1 ; 101) et ledit utilisateur via lesdits seconds moyens d'interface (4, 5), exécutables par lesdits premiers moyens logiciels (I, 20, 71) desdits premiers moyens de traitement de données (2 ; 29 ; 102),

* des moyens de protection dudit logiciel filtre (F, 62), pour empêcher toute lecture et/ou modification dudit logiciel filtre par une entité non autorisée, et

- l'un au moins desdits premiers et deuxièmes moyens de traitement de données (3 ; 29 , 30 ; 102 ; 130 ; Ssec) comprend un dispositif de traitement de données pour l'exécution dudit logiciel filtre (F, 62).

2. Terminal selon la revendication 1, caractérisé en ce que ledit dispositif d'exécution du logiciel filtre comprend des premiers moyens d'identification et /ou d'authentification de ladite application (Fap) implantée dans ladite unité électronique (Sap; PC) ou de l'origine desdites requêtes émises par ladite application.

3. Terminal selon la revendications 2, caractérisé en ce que ledit dispositif de traitement de données pour l'exécution dudit logiciel filtre (F, 62) comprend des moyens de vérification de l'intégrité des données reçues de ladite application (Fap).

4. Terminal selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit dispositif de traitement de données pour l'exécution dudit logiciel filtre (F, 62) comprend des moyens centralisés (Ssec) de contrôle des conditions d'utilisation des services du dispositif personnel de sécurité (31) en fonction de ladite application (Fap) et / ou de l'utilisateur.

5. Terminal selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit dispositif de traitement de données pour l'exécution dudit logiciel filtre (F, 62) comprend :

- des moyens pour commander le chargement sécurisé dudit logiciel filtre dans ladite mémoire programmable, via l'un desdits premiers ou troisièmes moyens d'interface, à partir d'une entité extérieure audit module, et

- des premiers moyens de contrôle d'accès pour n'autoriser ledit chargement dudit logiciel filtre qu'en réponse à au moins une condition prédéfinie.

6. Terminal selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comprend des deuxièmes moyens d'authentification desdits premiers moyens de traitement de données (2 ; 3 ; 29 ; Ssec) par lesdits deuxièmes moyens de traitement de données (30 ; 130).

7. Terminal selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comprend des troisièmes moyens d'authentification desdits deuxièmes moyens de traitement de données (30 ; 130) par lesdits premiers moyens de traitement de données (3 ; 29).

8. Terminal selon l'une quelconque des revendications 6 et 7, caractérisé en ce qu'il comprend un premier canal de communication (6) entre lesdits premiers (2 ; 3 ; 29) et deuxièmes (30 ; 130) moyens de traitement de données et des premiers moyens de sécurisation dudit premier canal de communication.

9. Terminal selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comprend des quatrièmes moyens d'authentification dudit module terminal (1 ; 101) par ledit utilisateur, indépendamment dudit dispositif personnel de sécurité (31 ; 131).

10. Terminal selon la revendication 9, caractérisé en ce que lesdits quatrièmes moyens d'authentification comprennent des moyens de calcul, par lesdits premiers moyens de traitement de données (2 ; 3 ; 29), et de présentation audit utilisateur, via lesdits deuxièmes moyens d'interface (4), d'un mot de passe connu dudit utilisateur et calculé sur la base d'au

moins un premier paramètre secret stocké dans lesdits premiers moyens de traitement de données (2 ; 3 ; 29).

11. Terminal selon l'une quelconque des revendications 1 à 10, caractérisé en ce qu'il comprend des cinquièmes moyens d'authèntification conjointe dudit module terminal (1 ; 101) et dudit dispositif personnel de sécurité (31 ; 131) par ledit utilisateur.

12. Terminal selon la revendication 11, caractérisé en ce que lesdits cinquièmes moyens d'authentification comprennent des moyens de calcul, par ledit dispositif d'exécution dudit logiciel filtre (3 ; 29 ; 31 ; 131), et de présentation audit utilisateur, via lesdits deuxièmes moyens d'interface (4), d'un mot de passe connu dudit utilisateur et calculé sur la base d'au moins un deuxième et un troisième paramètres secrets stockés en mémoire respectivement dans lesdits premiers (2 ; 3 ; 29) et deuxièmes (30 ; 130) moyens de traitement de données.

13. Terminal selon l'une quelconque des revendications 1 à 12, caractérisé en ce que ledit module terminal (1) comporte ladite mémoire programmable (3d) pour le chargement et le stockage dudit logiciel filtre (F, 62).

14. Terminal selon la revendication 13, caractérisé en ce que ledit logiciel filtre (F, 62) génère des premières commandes pour la mise en œuvre de ladite séquence d'échanges de données entre ledit module terminal (1) et ledit utilisateur, et en ce que lesdits premiers moyens de traitement de données comprennent un premier microprocesseur (2 ; 102) de pilotage desdits moyens d'interface (4-9) programmé grâce auxdits premiers moyens logiciels (20, 71) de pilotage desdits moyens d'interface pour exécuter lesdites premières commandes générées par ledit logiciel filtre (F, 62), et un deuxième microprocesseur sécurisé (3) du type pour carte à circuit intégré disposé dans ledit module terminal et comportant ladite mémoire programmable (3d), ledit second microprocesseur (3) exécutant ledit logiciel filtre (F, 62) pour le pilotage de ladite séquence d'échanges de données au moyen desdites premières commandes transmises audit premier microprocesseur (2) et pour l'application de ladite commande élémentaire ou séquence de commandes élémentaires auxdits deuxièmes moyens de traitement de données.

15. Terminal selon la revendication 14, caractérisé en ce que lesdits premiers moyens logiciels (20, 71) de pilotage des moyens d'interface comportent au moins un quatrième paramètre secret, ledit deuxième microprocesseur (3) étant commandé par ledit logiciel filtre (F, 62) pour authentifier lesdits premiers moyens logiciels (20, 71) de pilotage des moyens d'interface sur la base d'une information transmise par ledit premier microprocesseur (2) et combinée au moins avec ledit quatrième paramètre secret.

16. Terminal selon la revendication 15, caractérisé en ce qu'il comprend un deuxième canal de communication (12) entre lesdits premiers moyens logiciels (20, 71) de pilotage des moyens d'interface et ledit deuxième microprocesseur (3) et des deuxièmes moyens de sécurisation dudit deuxième canal de communication.

17. Terminal selon la revendication 16, caractérisé en ce que lesdits deuxièmes moyens de sécurisation comprennent des moyens de chiffrement et déchiffrement, par lesdits premiers moyens logiciels (20, 71) et par ledit deuxième microprocesseur (3), des données transmises sur ledit deuxième canal de communication (12), sur la base d'au moins un cinquième paramètre secret mémorisé dans lesdits premiers et deuxièmes moyens de traitement de données.

18. Terminal selon l'une quelconque des revendications 16 et 17, caractérisé en ce que lesdits deuxièmes moyens de sécurisation comprennent des premiers moyens physiques de protection dudit deuxième canal de communication (12) contre les intrusions.

19. Terminal selon l'une quelconque des revendications 15 à 18, caractérisé en ce que ledit premier microprocesseur (2) comporte une mémoire temporaire (2b) pour le stockage dudit paramètre secret et des deuxièmes moyens physiques de protection de ladite mémoire temporaire (2b) contre les intrusions.

20. Terminal selon l'une quelconque des revendications 14 à 19, caractérisé en ce que ledit deuxième microprocesseur (2) est un microcontrôleur.

21. Terminal selon la revendication 13, caractérisé en ce que ledit logiciel filtre génère des premières commandes pour la mise en œuvre de ladite séquence d'échanges de données entre ledit module terminal et ledit utilisateur et lesdits premiers moyens de traitement de données comprennent ledit dispositif d'exécution du logiciel filtre et sont constitués par un microprocesseur sécurisé (29) adapté pour :

* exécuter ledit logiciel filtre (F, 62) de traduction et de conversion desdites requêtes de haut niveau en au moins une séquence d'échanges de données entre le module terminal et l'utilisateur et/ou en au moins une commande élémentaire ou une séquence de commandes élémentaires exécutables par lesdits deuxièmes moyens logiciels desdits deuxièmes moyens de traitement de données (31),

* piloter lesdits moyens d'interface (4-9) grâce auxdites premières commandes générées par ledit logiciel filtre, pour la mise en œuvre de ladite séquence d'échanges entre ledit module terminal (1) et ledit utilisateur.

22. Terminal selon la revendication 21, caractérisé en ce que ledit microprocesseur (29) comporte ladite mémoire programmable.

23. Terminal selon la revendication 21, caractérisé en ce que ladite mémoire programmable est externe audit microprocesseur (29).

24. Terminal selon la revendication 23, caractérisé en ce que ledit logiciel filtre (F, 62) est stocké sous forme chiffrée dans ladite mémoire programmable et en ce que ledit microprocesseur (29) comprend des moyens pour lire, déchiffrer et exécuter ledit logiciel filtre.

25. Terminal selon l'une quelconque des revendications 14 à 24, caractérisé en ce que lesdits deuxièmes moyens de traitement de données dudit dispositif personnel de sécurité (31) comprennent un deuxième dispositif de traitement de données (30) pour l'exécution sécurisée d'un logiciel filtre et une mémoire programmable (30a) pour le chargement et le stockage dudit logiciel filtre (62), lesdits premiers moyens logiciels desdits premiers moyens de traitement de données étant adaptés pour recevoir lesdites commandes pour la mise en oeuvre de ladite séquence d'échange de données indifféremment de l'un ou l'autre desdits dispositifs (3 ; 29 ; 31) d'exécution de logiciel filtre implantés dans ledit module et ledit dispositif personnel de sécurité respectivement.

26. Terminal selon l'une quelconque des revendications 13 à 25, caractérisé en ce que :

- ledit logiciel filtre (F, 62) comprend au moins un paramètre secret,

- lesdits deuxièmes moyens de traitement (30) de données comprennent des seconds moyens de contrôle d'accès conditionnels pour n'autoriser l'exécution desdits calculs cryptographiques, en réponse à des commandes élémentaires générées par ledit logiciel filtre (F, 62), que si au moins une seconde condition prédéfinie, fonction dudit paramètre secret est remplie.

27. Terminal selon l'une quelconque des revendications 1 à 12, caractérisé en ce que ledit dispositif personnel de sécurité (131) comporte ladite mémoire programmable (130a) pour le chargement et le stockage dudit logiciel filtre (F, 62).

28. Terminal selon la revendication 27, caractérisé en ce que ledit logiciel filtre (F, 62) génère des premières commandes pour la mise en œuvre de ladite séquence d'échanges de données entre ledit module terminal (1) et ledit utilisateur et ce que lesdits premiers moyens de traitement de données comprennent un premier microprocesseur (2 ; 102) de pilotage desdits moyens d'interface (4-9), programmé grâce auxdits premiers moyens logiciels (20, 71), pour exécuter lesdites premières commandes, générées par ledit logiciel filtre (F,62), et lesdits deuxièmes moyens de traitement de données comprennent un deuxième microprocesseur sécurisé (130) du type pour carte à circuit intégré disposé dans ledit dispositif personnel de sécurité (131) et comportant ladite mémoire programmable (130a), ledit second microprocesseur (130) exécutant (i) ledit logiciel filtre (F, 62) pour le pilotage de ladite séquence d'échanges de données au moyen desdites premières commandes

transmises audit premier microprocesseur (2 ; 102), ainsi que (ii) lesdites commandes élémentaires.

29. Terminal selon les revendications 6 et 28, caractérisé en ce que lesdits premiers moyens logiciels (20, 71) de pilotage desdits moyens d'interface comportent au moins un paramètre secret et ledit second microprocesseur (130) dudit dispositif personnel de sécurité (131) est commandé par ledit logiciel filtre (62) pour authentifier ledit premier microprocesseur (2) sur la base d'une information transmise par ledit premier microprocesseur (2) et combinée au moins avec ledit paramètre secret.

30. Terminal selon l'une quelconque des revendications 28 et 29, caractérisé en ce que ledit deuxième microprocesseur (130) dudit dispositif personnel de sécurité (131) est adapté pour commander le chargement dudit logiciel filtre (F, 62) dans ladite mémoire programmable (130a) via lesdits premiers moyens d'interface (7-9) et lesdits troisièmes moyens (6) d'interface avec ledit dispositif personnel de sécurité (131).

31. Terminal selon l'une quelconque des revendications 13 à 30, caractérisé en ce que ledit module terminal (1 ; 101) est constitué par un lecteur de carte à circuit intégré et ledit dispositif personnel de sécurité est une carte à circuit intégré (31 ; 131).

32. Terminal selon la revendication 13, caractérisé en ce que ledit module terminal (1) comprend un ordinateur personnel (102) et en ce que ladite mémoire reprogrammable est constituée par le disque dur (102b) dudit ordinateur.

33. Terminal selon la revendication 32 et l'une quelconque des revendications 14 à 17, caractérisé en ce que ledit premier microprocesseur est constitué par le microprocesseur (102c) dudit ordinateur personnel (102), ledit ordinateur personnel (102) étant en outre interfacé audit microprocesseur sécurisé (3).

34. Terminal selon la revendication 32, caractérisé en ce que ledit logiciel filtre (F) comprend un premier module de chargement/déchiffrement (Fcd) et un deuxième module chiffré (Fchi) pour ladite traduction des requêtes de haut niveau, ledit premier module (Fcd) commandant le chargement dudit deuxième module (Fchi) en mémoire RAM dudit ordinateur (102) et son déchiffrement pour l'exécution dudit logiciel filtre par ledit ordinateur.

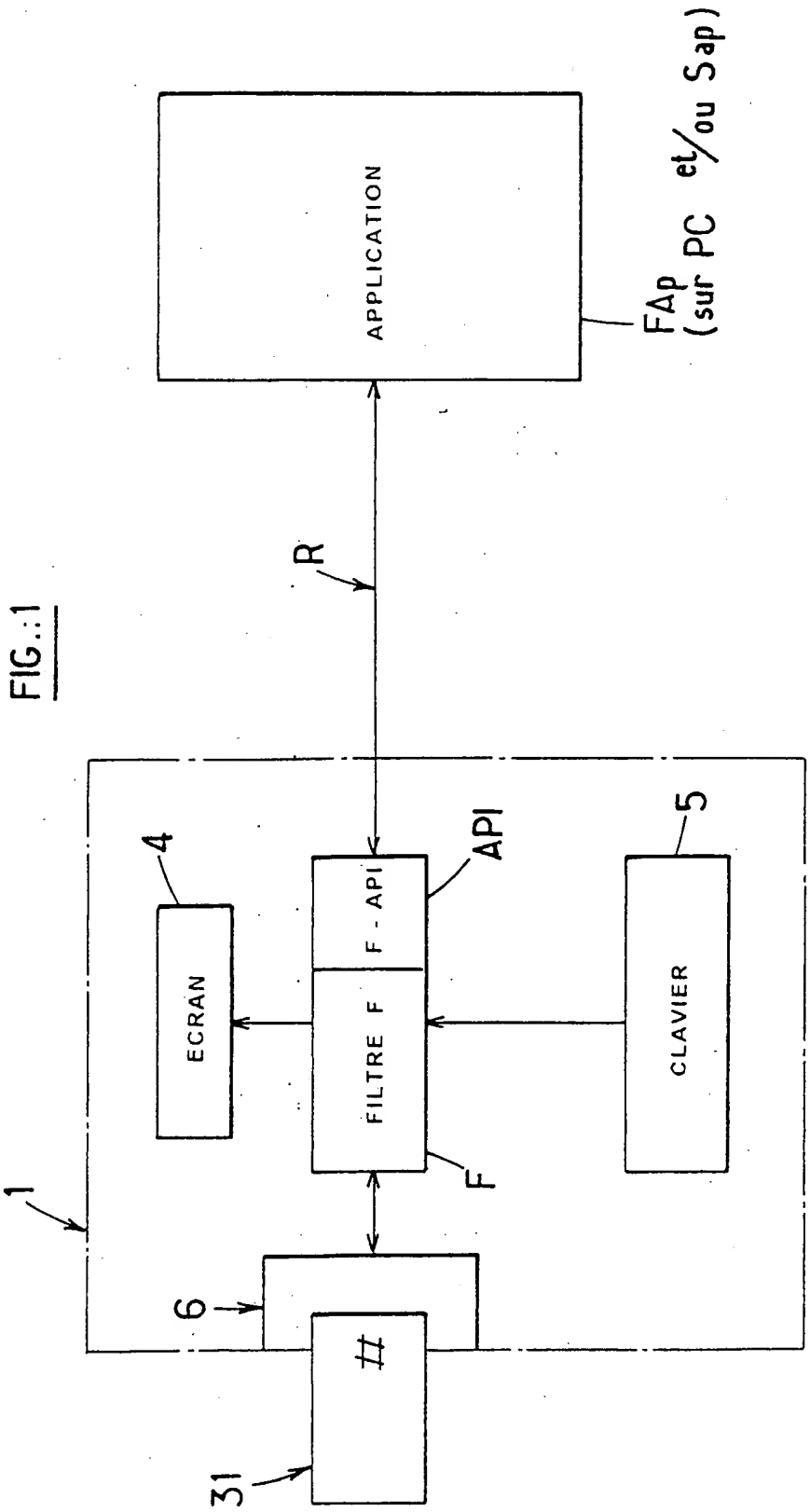
35. Terminal selon la revendication 32, caractérisé en ce que ledit logiciel filtre (F) comprend au moins un premier module (F-PC) implanté sur ledit ordinateur personnel (102) et au moins un deuxième module (F-SE) implanté sur un serveur de sécurité (Ssec), ledit ordinateur personnel (102) et ledit serveur de sécurité (Ssec) étant connectés par un canal de communication sécurisé (CS) permettant un échange de données protégé entre lesdits modules.

36. Terminal selon l'une quelconque des revendications 32 à 35, caractérisé en ce que ledit dispositif personnel de sécurité (31) est une carte à circuit intégré.

37. Système pour la mise en œuvre de transactions sécurisée, caractérisé en ce qu'il comprend au moins un terminal (1, 31 ; 101, 131) selon l'une quelconque des revendications 1 à 36, et au moins une unité électronique (Sap ; PC) comportant des moyens pour transmettre lesdites requêtes de haut niveau audit terminal (1, 31 ; 101, 131).

38. Système selon la revendication 37, caractérisé en ce qu'il comprend une pluralité de terminaux (1, 31 ; 101, 131), au moins un serveur (S) constituant ladite unité électronique, et des moyens (CR) de transmission de données numériques entre ledit serveur (S) et lesdits terminaux.

FIG.:1


APPLICATION
FAp (sur PC et/ou Sap)
R
API
F - API
FILTRE F
F
ECRAN
4
CLAVIER
5
1
6
#
31

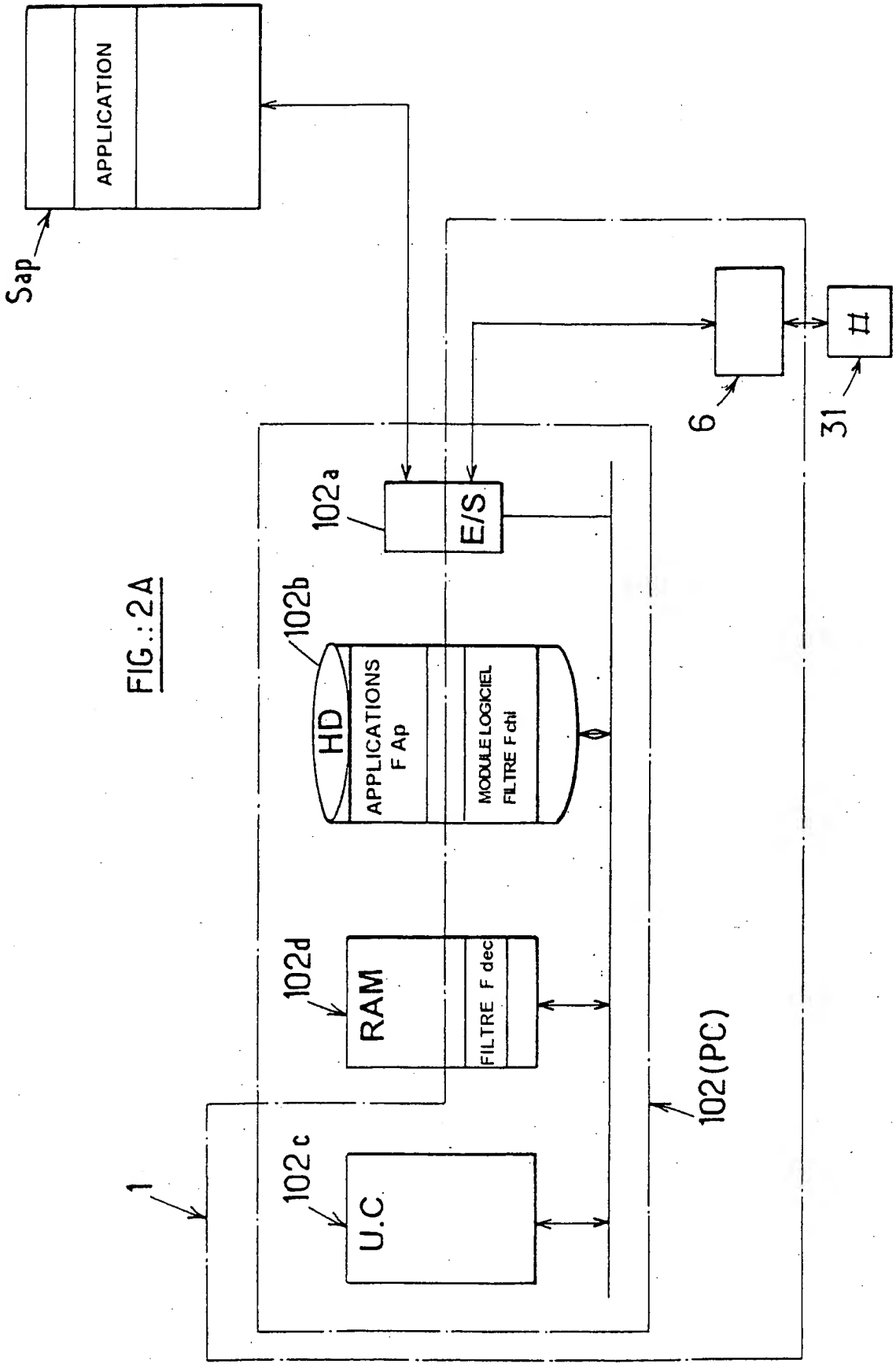

APPLICATION
Sap
6
31
102a
E/S
102b
HD
APPLICATIONS
F Ap
MODULE LOGICIEL
FILTRE F chl
102d
RAM
FILTRE F dec
102c
U.C
1
102(PC)

FIG.: 2A

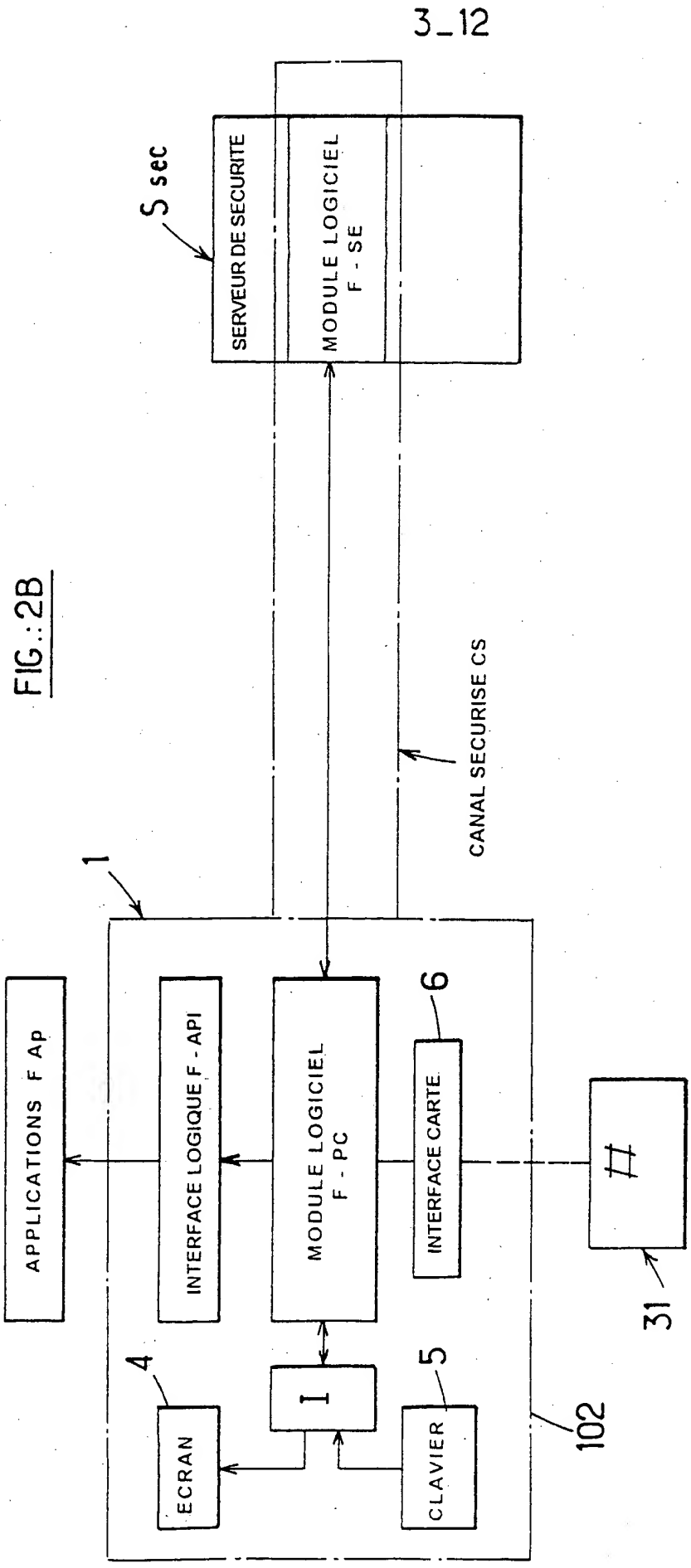

3_12
S sec
SERVEUR DE SECURITE
MODULE LOGICIEL F - SE
CANAL SECURISE CS
1
APPLICATIONS F Ap
INTERFACE LOGIQUE F - API
MODULE LOGICIEL F - PC
6
INTERFACE CARTE
#
31
4
ECRAN
I
5
CLAVIER
102

FIG.:2B

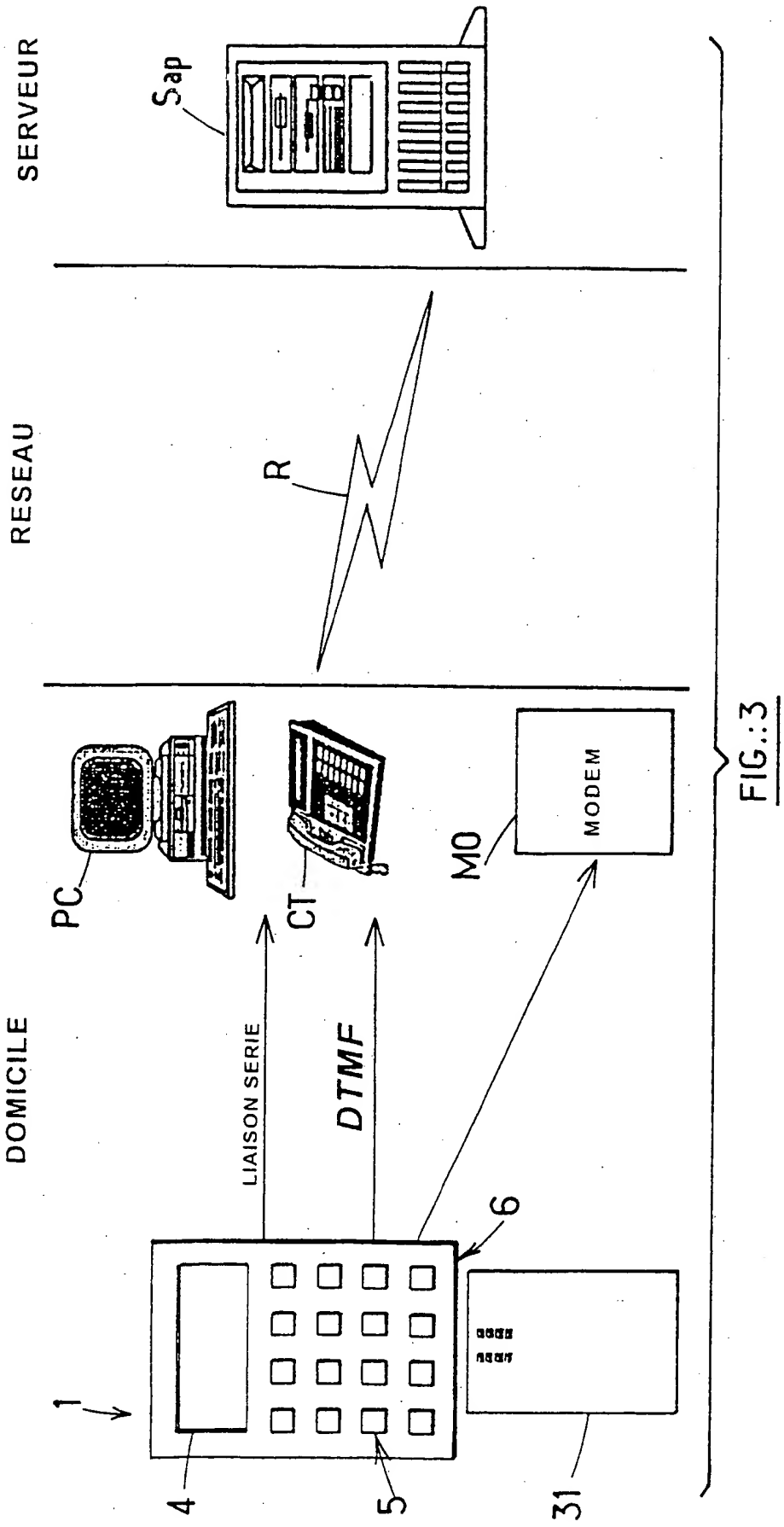

SERVEUR
Sap
RESEAU
R
DOMICILE
PC
CT
MO
MODEM
LIAISON SERIE
DTMF
6
1
4
5
31

FIG.:3

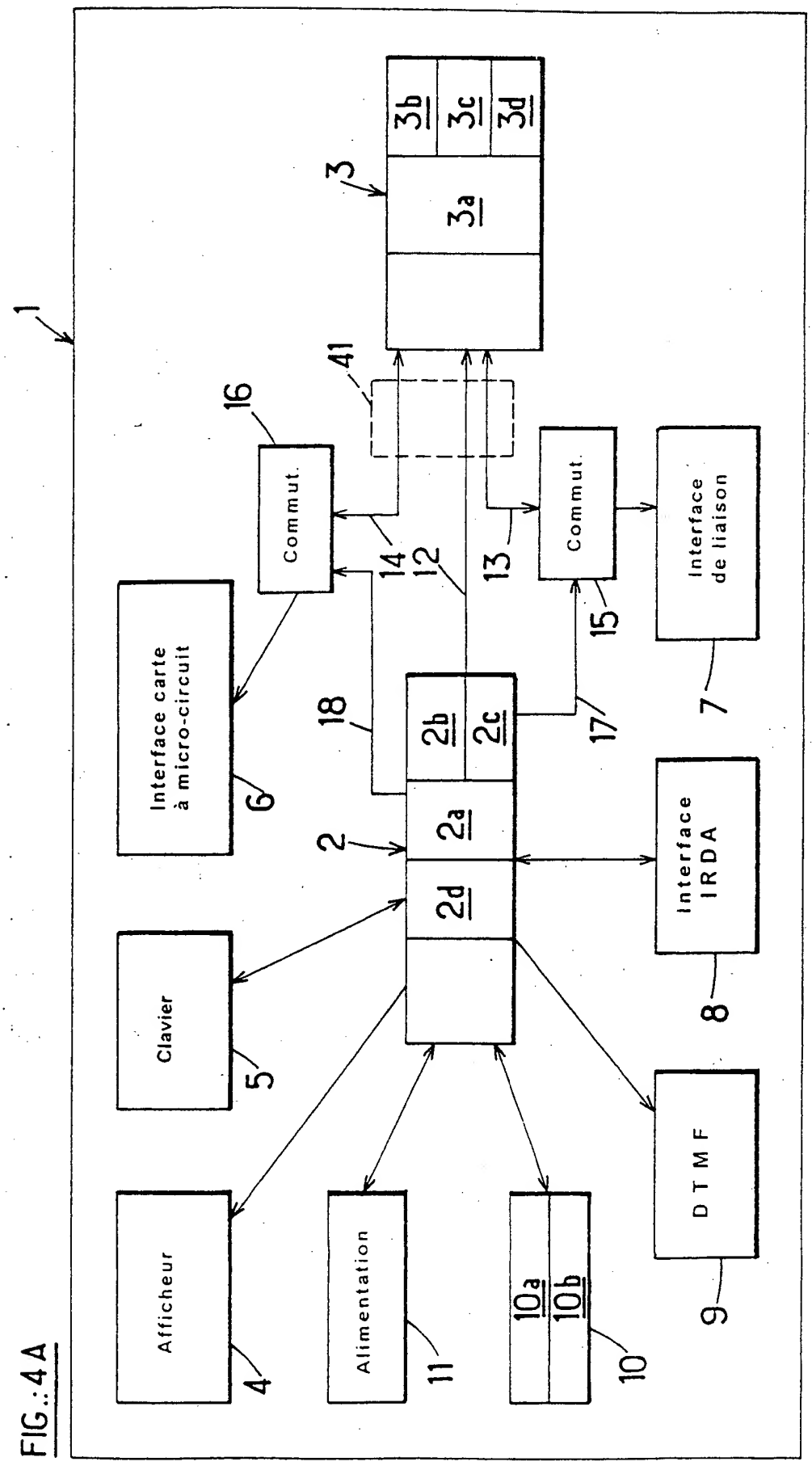

1
3
3a
3b
3c
3d
41
16
Commut.
14
12
13
Commut.
15
Interface de liaison
7
Interface carte à micro-circuit
6
18
2
2a
2b
2c
2d
17
Interface IRDA
8
Clavier
5
DTMF
9
Afficheur
4
Alimentation
11
10a
10b
10

FIG.:4A

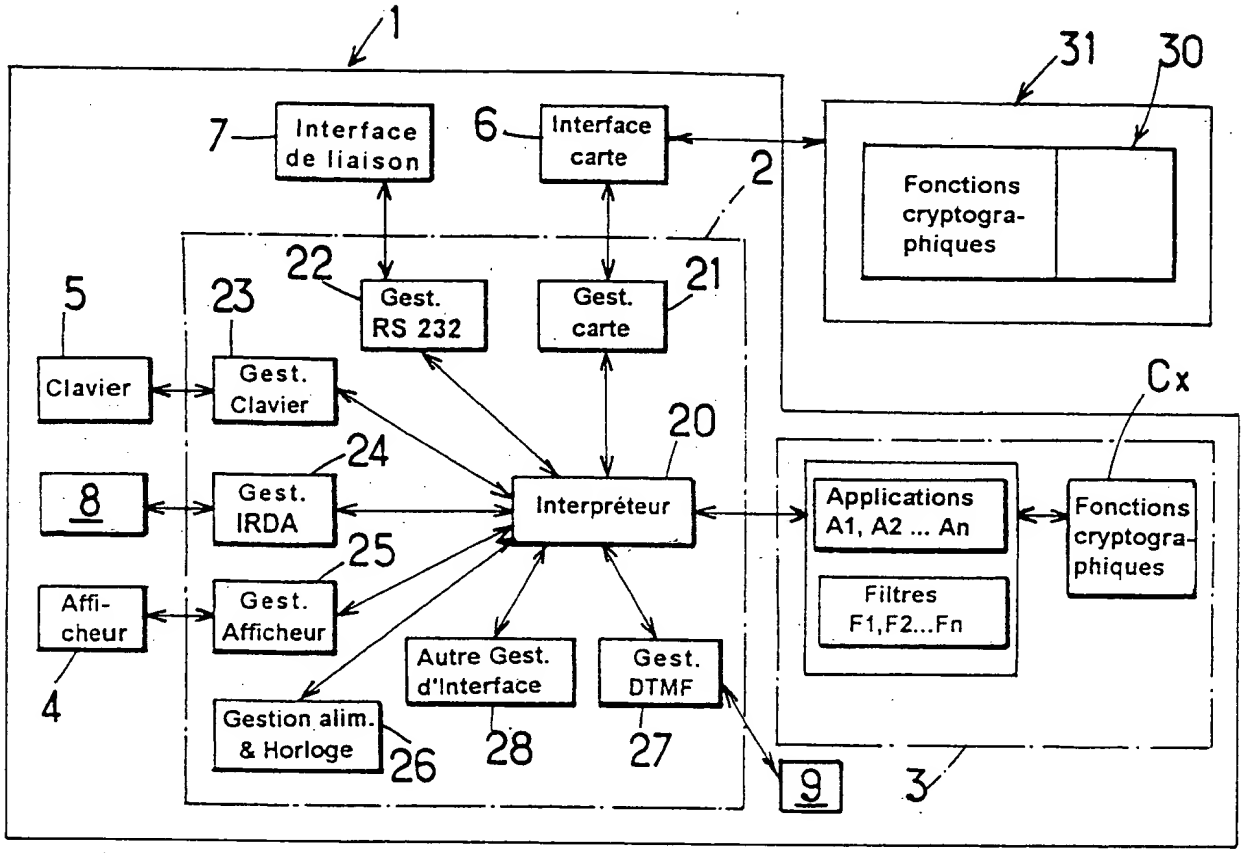
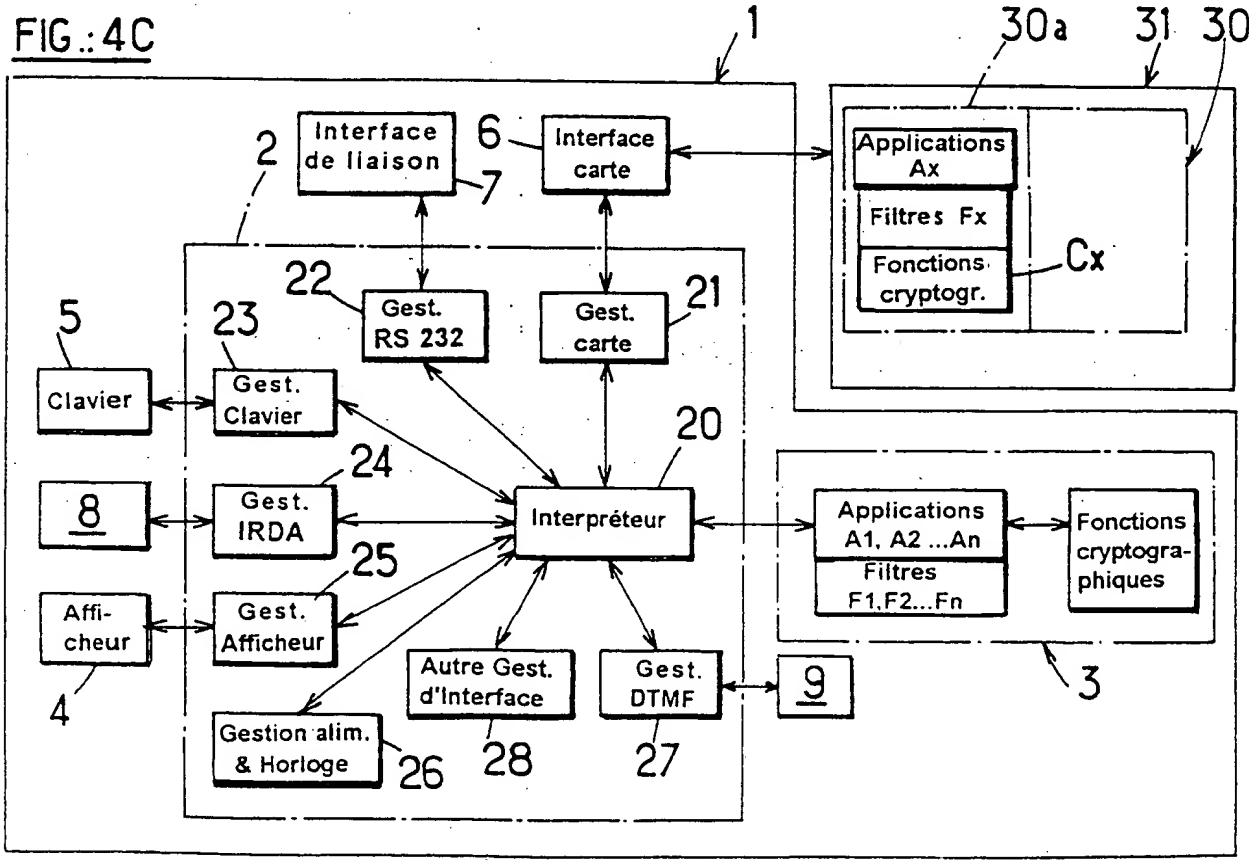

1
31
30
7
Interface de liaison
6
Interface carte
2
Fonctions cryptogra-phiques
22
Gest. RS 232
Gest. carte
21
5
23
Clavier
Gest. Clavier
Cx
20
24
8
Gest. IRDA
Interpréteur
Applications A1, A2 ... An
Fonctions cryptogra-phiques
25
Affi-cheur
Gest. Afficheur
Filtres F1,F2...Fn
Autre Gest. d'Interface
Gest. DTMF
4
Gestion alim. & Horloge
26
28
27
9
3

FIG.: 4B

FIG.: 4C


1
30a
31
30
Interface de liaison
2
6
Interface carte
7
Applications Ax
Filtres Fx
Fonctions cryptogr.
Cx
22
Gest. RS 232
Gest. carte
21
5
23
Clavier
Gest. Clavier
20
24
8
Gest. IRDA
Interpréteur
Applications A1, A2 ...An
Fonctions cryptogra-phiques
25
Affi-cheur
Gest. Afficheur
Filtres F1,F2...Fn
Autre Gest. d'Interface
Gest. DTMF
9
4
Gestion alim. & Horloge
26
28
27
3

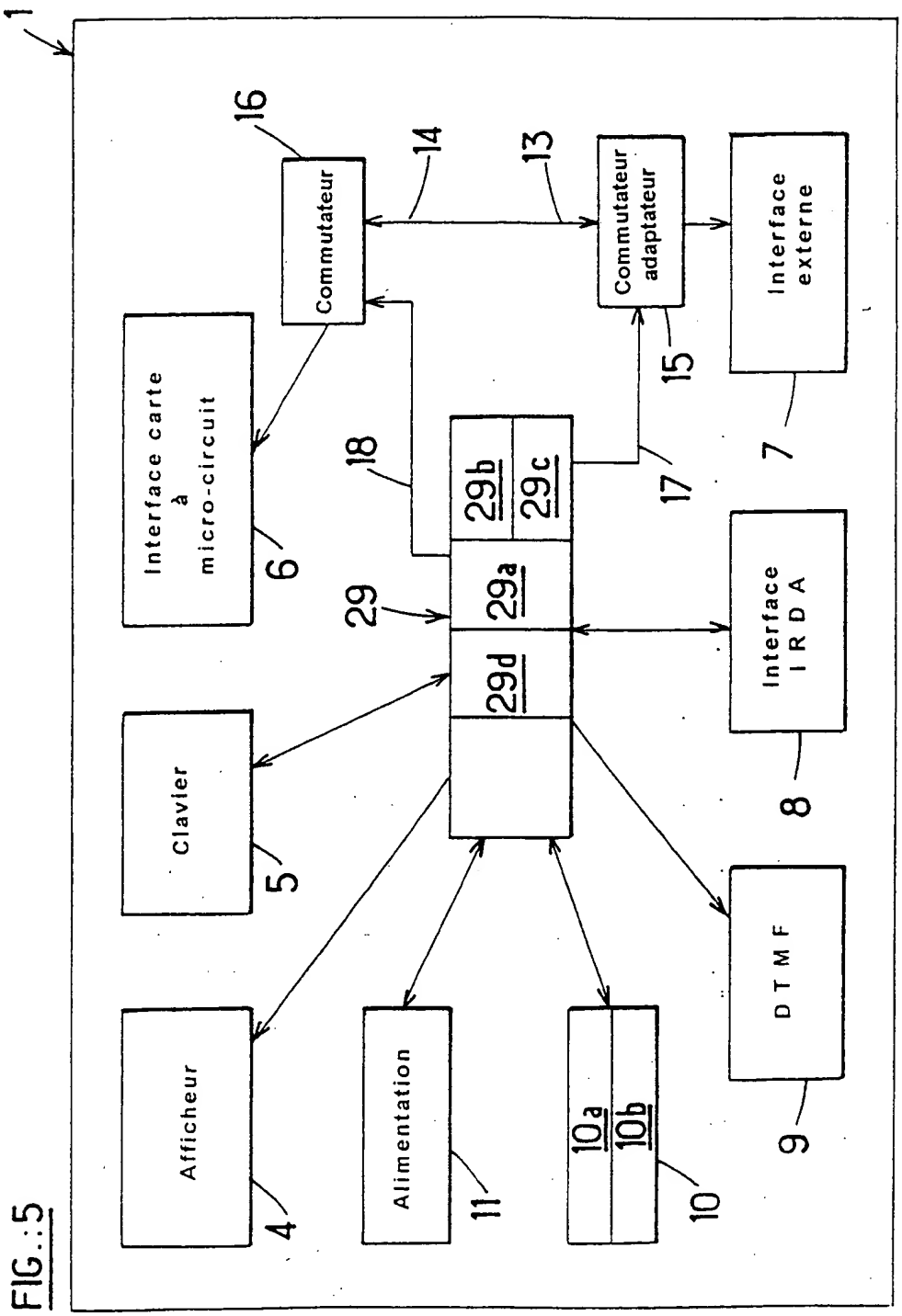

1
16
Commutateur
14
13
Commutateur adaptateur
Interface externe
Interface carte à micro-circuit
6
18
29b
29c
17
15
7
29
29a
29d
Interface I R D A
8
Clavier
5
D T M F
9
Afficheur
4
Alimentation
11
10a
10b
10

FIG.:5

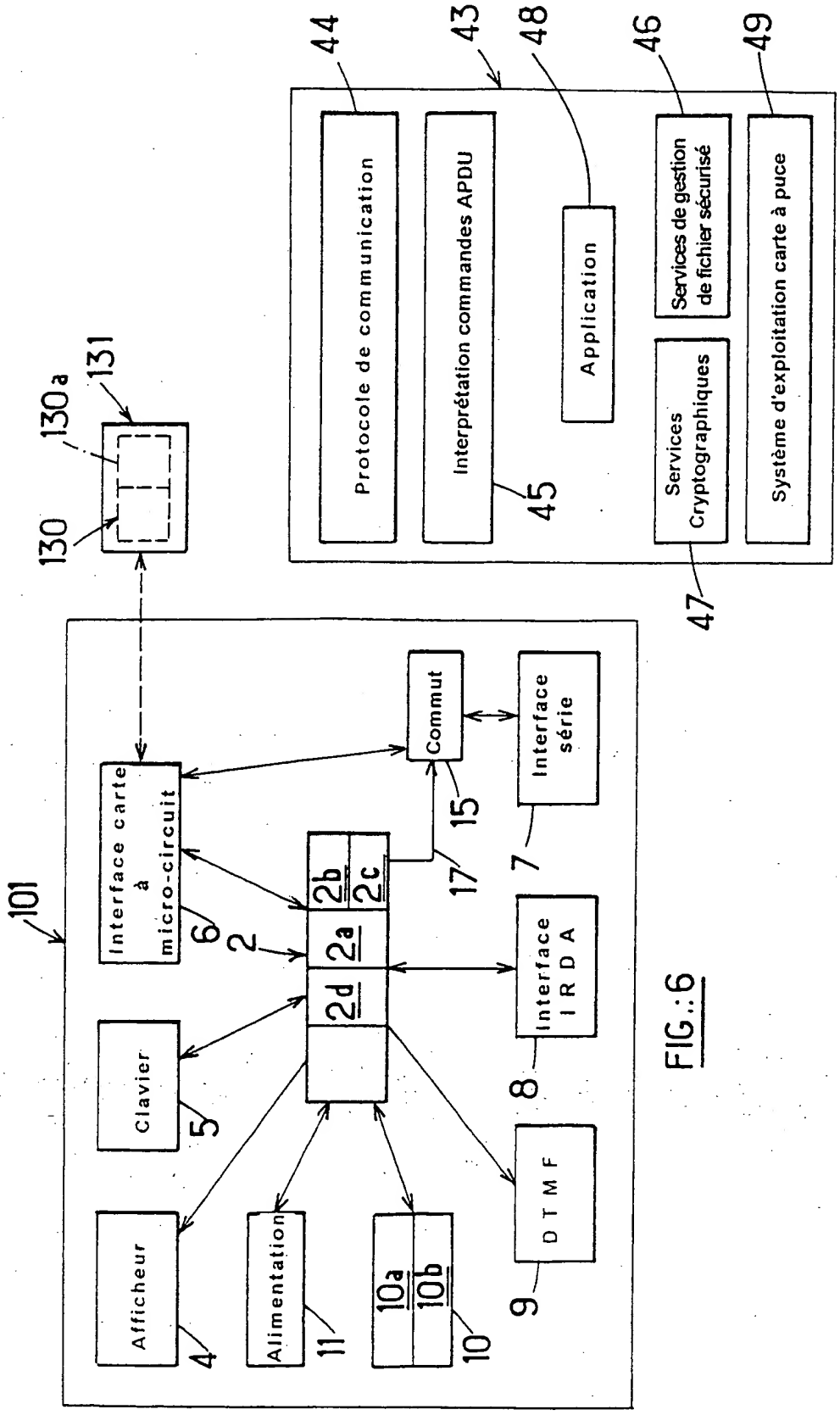

101
130
130a
131
Interface carte à micro-circuit
6
Clavier
5
Afficheur
4
Alimentation
11
10a
10b
10
2
2a
2b
2c
2d
Commut
15
17
Interface série
7
Interface IRDA
8
DTMF
9
44
43
48
46
49
Protocole de communication
Interprétation commandes APDU
45
Application
Services de gestion de fichier sécurisé
Services Cryptographiques
Système d'exploitation carte à puce
47

FIG.:6

FIG.:7

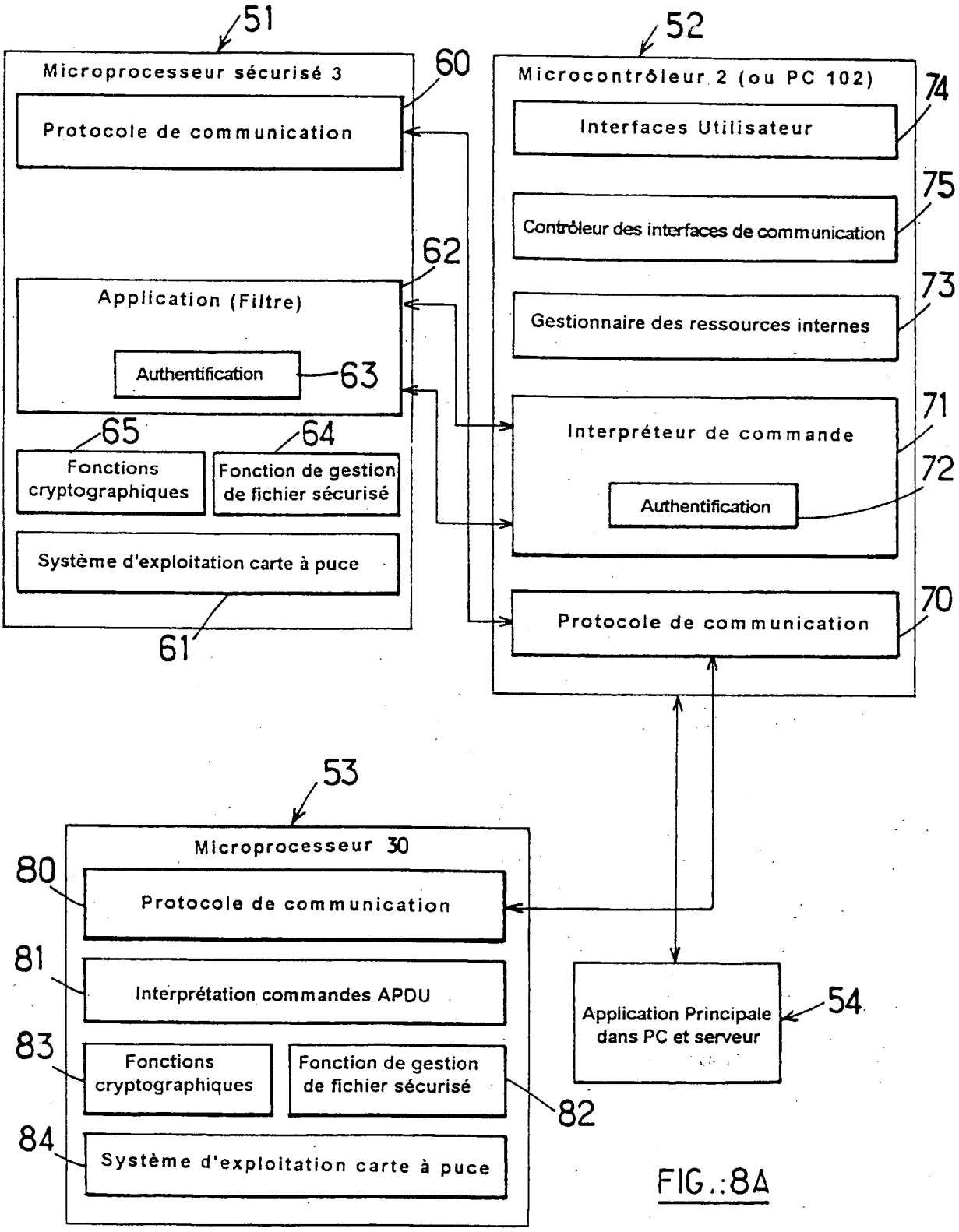

51
Microprocesseur sécurisé 3
60
Protocole de communication
62
Application (Filtre)
Authentification
63
65
Fonctions cryptographiques
64
Fonction de gestion de fichier sécurisé
Système d'exploitation carte à puce
61
52
Microcontrôleur 2 (ou PC 102)
74
Interfaces Utilisateur
75
Contrôleur des interfaces de communication
73
Gestionnaire des ressources internes
71
Interpréteur de commande
72
Authentification
70
Protocole de communication
53
Microprocesseur 30
80
Protocole de communication
81
Interprétation commandes APDU
83
Fonctions cryptographiques
Fonction de gestion de fichier sécurisé
82
84
Système d'exploitation carte à puce
Application Principale dans PC et serveur
54

FIG.:8A

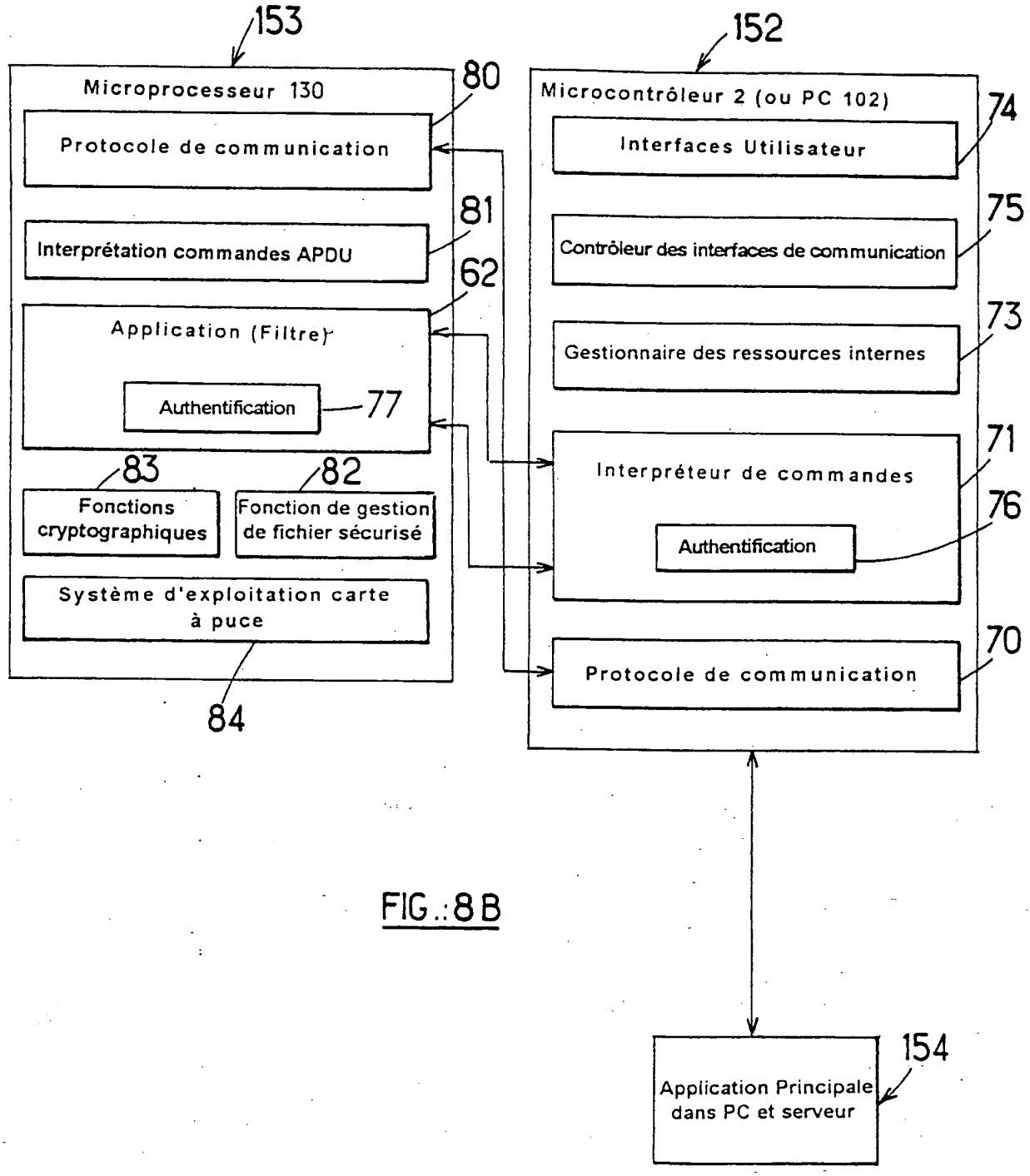

153
Microprocesseur 130
80
Protocole de communication
81
Interprétation commandes APDU
62
Application (Filtre)
Authentification
77
83
Fonctions cryptographiques
82
Fonction de gestion de fichier sécurisé
Système d'exploitation carte à puce
84
152
Microcontrôleur 2 (ou PC 102)
74
Interfaces Utilisateur
75
Contrôleur des interfaces de communication
73
Gestionnaire des ressources internes
71
Interpréteur de commandes
76
Authentification
70
Protocole de communication
154
Application Principale dans PC et serveur

FIG.:8B

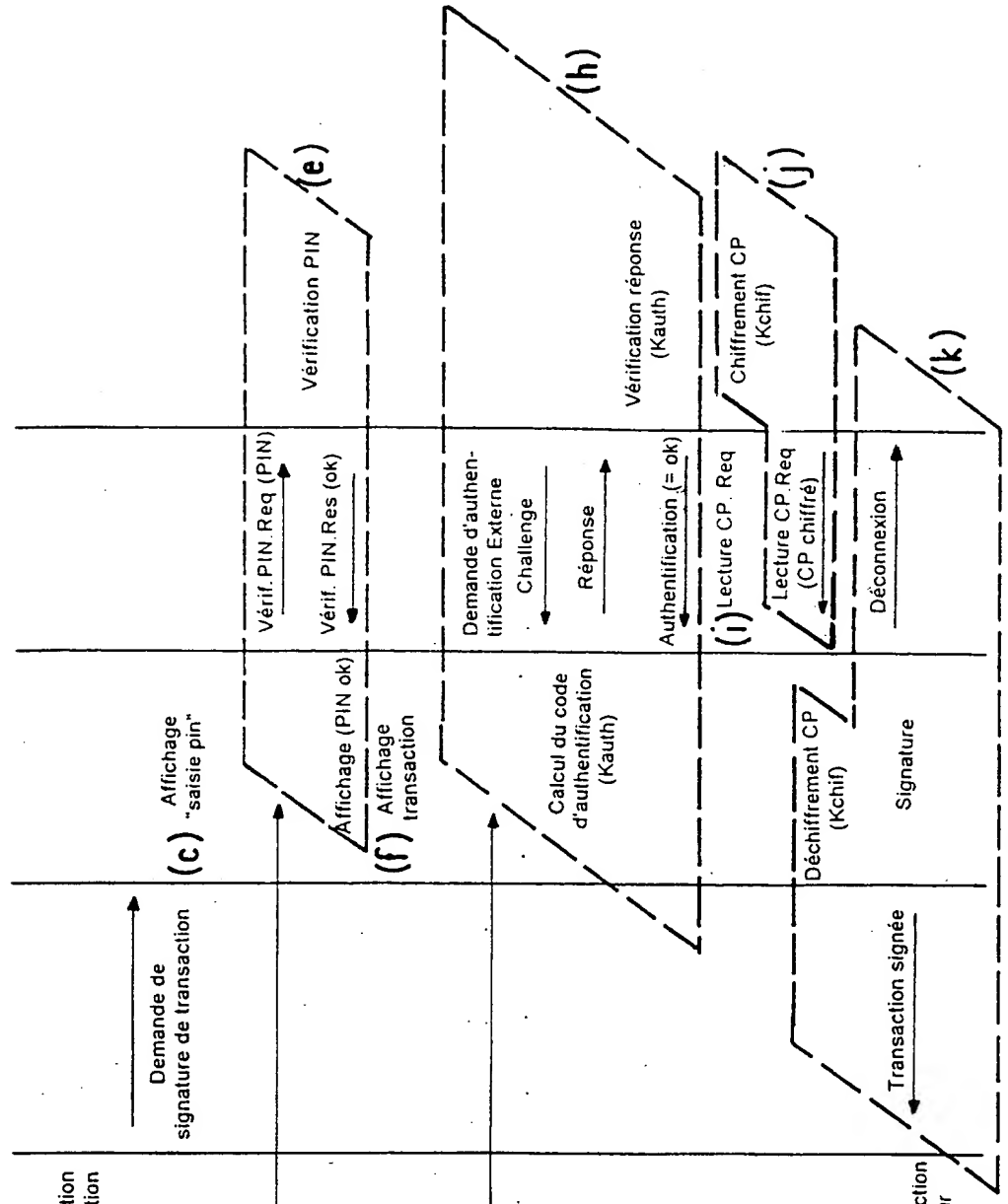

Utilisateur
Ordinateur PC
Module Terminal 1
Carte 31
(a) Constitution commandes
Commandes
(b) Elaboration transaction
Demande de signature de transaction
(c) Affichage "saisie pin"
(d) Saisie du PIN sur le clavier 5
Vérif.PIN.Req (PIN)
Vérif. PIN.Res (ok)
Vérification PIN
(e)
Affichage (PIN ok)
(f) Affichage transaction
(g) Validation transaction
Demande d'authentification Externe
Challenge
Réponse
Calcul du code d'authentification (Kauth)
Vérification réponse (Kauth)
(h)
Authentification (= ok)
(i) Lecture CP. Req
Chiffrement CP (Kchif)
(j)
Lecture CP.Req (CP chiffré)
Déchiffrement CP (Kchif)
Signature
Déconnexion
(k)
Transaction signée
Envoi transaction au serveur

FIG. : 9

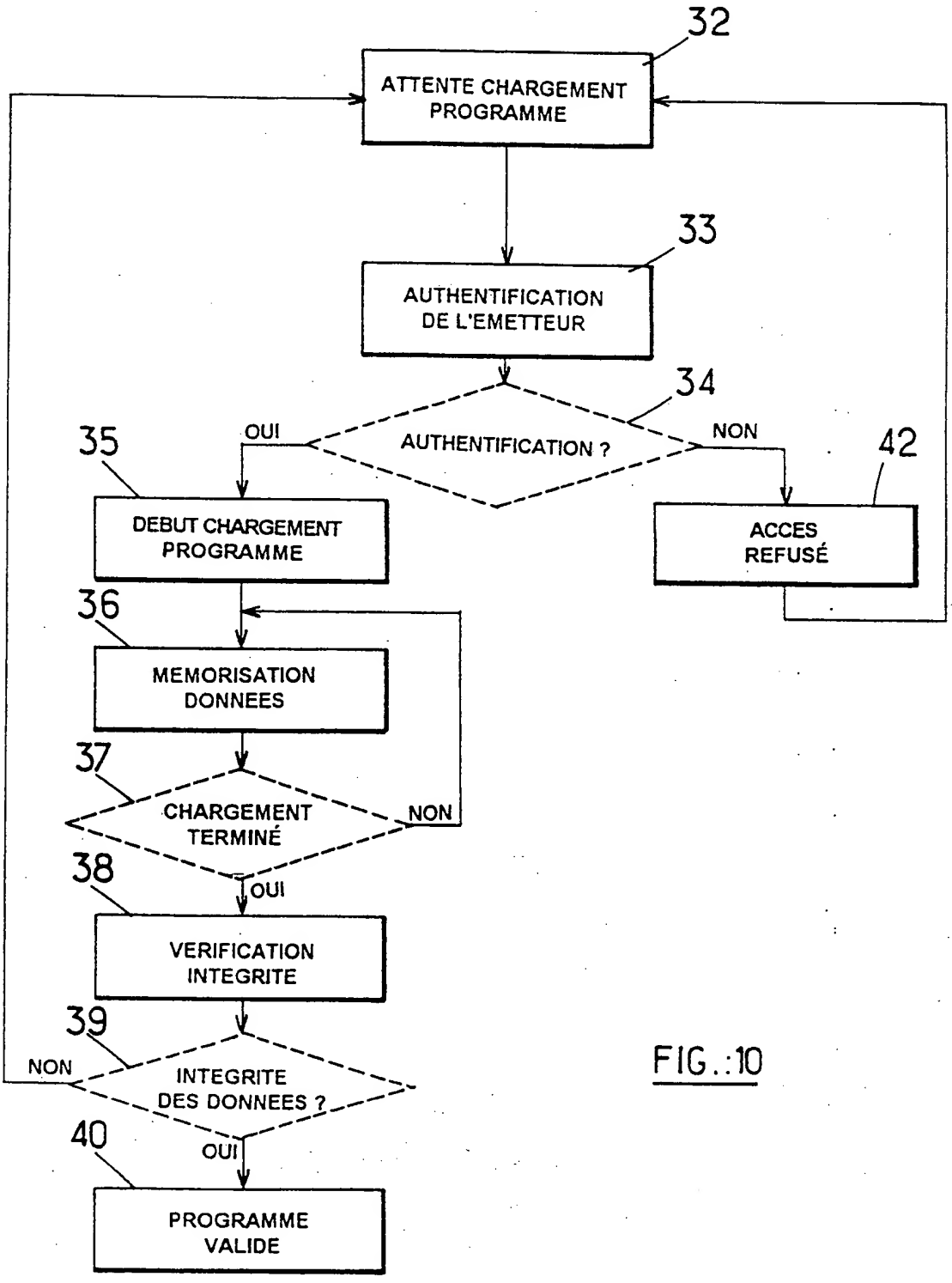

32
ATTENTE CHARGEMENT PROGRAMME
33
AUTHENTIFICATION DE L'EMETTEUR
34
AUTHENTIFICATION ?
OUI
NON
35
DEBUT CHARGEMENT PROGRAMME
42
ACCES REFUSÉ
36
MEMORISATION DONNEES
37
CHARGEMENT TERMINÉ
NON
OUI
38
VERIFICATION INTEGRITE
39
INTEGRITE DES DONNEES ?
NON
OUI
40
PROGRAMME VALIDE

FIG.:10

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/FR 99/01202

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 50207 A (TELIA AB PUBL) 31 December 1997 (1997-12-31) claim 1; figure 1 ---	1-38
A	US 5 446 864 A (BURGHARDT MARTIN ET AL) 29 August 1995 (1995-08-29) claim 1; figure 1 ---	1-38
A	US 4 442 484 A (CHILDS JR ROBERT H E ET AL) 10 April 1984 (1984-04-10) claim 1; figure 1 ---	1-38
A	WO 95 04328 A (INTELLECT AUSTRALIA PTY LTD ;OLIVER QUENTIN REES (AU); BERTINA JOH) 9 February 1995 (1995-02-09) cited in the application claim 1; figure 2 --- -/--	1-38

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 August 1999	10/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

1

INTERNATIONAL SEARCH REPORT

Inte. onal Application No
PCT/FR 99/01202

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 29667 A (SANDBERG DIMENT ERIK) 26 September 1996 (1996-09-26) claim 1; figure 1	1-38

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ..ional Application No
PCT/FR 99/01202

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9750207 A	31-12-1997	SE 509033 C	30-11-1998
		EP 0906680 A	07-04-1999
		NO 985951 A	24-02-1999
		SE 9602528 A	27-12-1997
US 5446864 A	29-08-1995	WO 9310498 A	27-05-1993
US 4442484 A	10-04-1984	NONE	
WO 9504328 A	09-02-1995	AU 7341894 A	28-02-1995
		CA 2168434 A	02-09-1995
		EP 0711441 A	15-05-1996
WO 9629667 A	26-09-1996	US 5826245 A	20-10-1998
		AU 5366096 A	08-10-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Den .e internationale No
PCT/FR 99/01202

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de donnees. et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec. le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 97 50207 A (TELIA AB PUBL) 31 décembre 1997 (1997-12-31) revendication 1; figure 1	1-38
A	US 5 446 864 A (BURGHARDT MARTIN ET AL) 29 août 1995 (1995-08-29) revendication 1; figure 1	1-38
A	US 4 442 484 A (CHILDS JR ROBERT H E ET AL) 10 avril 1984 (1984-04-10) revendication 1; figure 1	1-38
A	WO 95 04328 A (INTELLECT AUSTRALIA PTY LTD ;OLIVER QUENTIN REES (AU); BERTINA JOH) 9 février 1995 (1995-02-09) cité dans la demande revendication 1; figure 2	1-38

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
3 août 1999	10/08/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets. P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

1

RAPPORT DE RECHERCHE INTERNATIONALE

Den ...ie internationale No
PCT/FR 99/01202

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 96 29667 A (SANDBERG DIMENT ERIK) 26 septembre 1996 (1996-09-26) revendication 1; figure 1	1-38

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Der. de internationale No
PCT/FR 99/01202

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9750207	A	31-12-1997	SE	509033 C	30-11-1998
			EP	0906680 A	07-04-1999
			NO	985951 A	24-02-1999
			SE	9602528 A	27-12-1997
US 5446864	A	29-08-1995	WO	9310498 A	27-05-1993
US 4442484	A	10-04-1984	AUCUN		
WO 9504328	A	09-02-1995	AU	7341894 A	28-02-1995
			CA	2168434 A	02-09-1995
			EP	0711441 A	15-05-1996
WO 9629667	A	26-09-1996	US	5826245 A	20-10-1998
			AU	5366096 A	08-10-1996

56

VERIFICATION OF A TRANSLATION

*I, **Jean-Pierre COLAS***

Patent Attorney of Cabinet de BOISSE et COLAS, 37 Avenue Franklin D. Roosevelt, 75008 PARIS, France,

hereby declare that I am fully conversant with the French and English languages, and

certify that, to the best of my knowledge and belief, the attached English specification is a true and complete translation of the international Application No. PCT/FR99/01202 as filed and published under No. WO 99/62037 on December 2, 1999.

Signed at Paris, France
this 17th December, 1999

Jean-Pierre COLAS

The present invention concerns a terminal and a system for performing secure electronic transactions.

Public digital data transmission networks, such as the Internet, are expanding at a considerable rate. However, the performing of secure electronic transfers on this type of network is currently being hampered, among other things, by the lack of security mechanisms associated with such transactions, reflected in a lack of confidence on the part of network users and operators.

In the context of this application:

- an electronic transaction designates an exchange of information via a public digital data transmission or telecommunication network, either between two or more users or between a user and a service provider,

- a function is a process carried out in order to render a service to a user,

- an application designates a consistent set of services and functions,

- the expression "application software" designates the software needed to perform the functions relating to a given application, and

- a secure transaction is a transaction for which security measures are implemented, namely authentication of the entities participating in the transaction, integrity, confidentiality, authenticity and possibly non-repudiation of exchanges and operations effected in the context of the transaction.

Many applications require secure electronic transactions. Examples are controlling access to computer or similar resources, home banking (statements, transfers between accounts, etc ... via the telephone network or the Internet), electronic trading (purchase of goods or services via a public network), electronic mail, electronic purse, etc.

These and other applications requiring secure transactions are well known to the skilled person and are not described in detail here.

Depending on their nature, rendering such applications secure necessitates the use of one or more security services such as:

- authentication, to guarantee the identity of an entity (a person or a system);

- access control, protecting against unauthorised use or manipulation of resources;

- confidentiality, prohibiting disclosure of data to unauthorised entities;

- data integrity, which assures that data has not been modified, deleted or substituted without authorisation, and

- non-repudiation, which assures that a participant in an exchange of data cannot

subsequently deny the existence of the exchange.

The combination of two existing techniques makes it feasible to employ the above security services, so offering a sufficient level of security for the performance of electronic transactions.

These are:

- public key and private key cryptography, because it guarantees non-repudiation and facilitates management of keys; and

- the integrated circuit card (or smart card), because it is relatively inexpensive, easy to use and reliable because it uses dedicated microprocessors with hardware and software protection features so that read and write mode access to their memory can be barred.

Integrated circuit cards offer the following services:

* authentication of the cardholder or user: this operation authenticates the cardholder by means of a confidential code after which the card allows operations such as executing algorithms, reading secret keys, reading or writing data on the card, which can also be subject to other security conditions;

* protection of data and functions stored on the integrated circuit card. Access to the card can be subject to prior authentication of the electronic entity requesting to access it. This external authentication is generally effected in challenge/response mode. In this case the entity has a secret parameter, hereinafter also called the secret, enabling it to calculate, depending on a challenge issued by the card, a response that will prove to the card that it is in possession of the secret;

* execution of cryptographic algorithms using a secret parameter stored on the card (encipherment, message authentication, signature); and

* internal authentication. This service enables an application to authenticate the card. This service is the inverse of external authentication. The card generates a response to a challenge received and a secret stored on the card.

The services offered by means of the integrated circuit card are performed on receipt of so-called elementary commands, execution of the elementary command causing the sending of elementary responses. The elementary commands concern, for example, cryptographic calculations, reading or writing of secret or other data, intervention of the user (entry of their personal confidential code (PIN), validation of a transaction after signature), and return of information to the user (display of messages to be signed, for example).

Some cards offer the facility to verify the integrity, source and even the confidentiality of

commands sent to the card. These services are based on techniques of authenticating and enciphering the commands.

The current use of integrated circuit (or microcircuit) cards offers a very high level of security because the transactions are essentially performed on private networks and terminals (automatic teller machines, point of sale terminals, for example) which are under the control of an entity assuring the security of the system as a whole.

In such applications, users or abusers do not have access to the application software or to the hardware and software security mechanisms of the terminals.

In contrast, performing secure transactions using integrated circuit cards on a public network presupposes that users have access to a card reader terminal module, given that microcircuit cards do not have their own electrical power supply and that using them requires a reader that can power them up and establish communication with the user and/or external electronic means.

At present, to perform a transaction on a public network, the user employs a terminal that can be a dedicated product, a personal computer or a personal computer connected to an integrated circuit card by a card reader.

In all cases, the transaction system accessible to the user generally comprises:

- an application service provider, for example an Internet browser, an electronic mail program, a home banking program,
- a high-level security service provider enabling execution of low-level cryptographic mechanisms required by the application.

The application service provider issues requests for high-level security services to assure the security of the transactions performed.

If the application is installed on the user's personal computer, the cryptographic services referred to are, for example, those defined by RSA laboratories in its standard "PKCS 11 : Cryptographic Token Interface Standard" or the cryptographic services offered by the Microsoft Windows NT operating system, in particular those available via the "Crypto API" application program interface (API).

If the user does not have an integral microcircuit card reader, the cryptographic services are effected entirely by software.

If the user wishes to enhance security, they use a transparent type integrated circuit card reader connected to their computer. A transparent type card reader is in fact an interface module between the computer and the integrated circuit card for transmitting elementary

commands from the computer, originating from the cryptographic service provider, to the card, and elementary responses from the card to the computer. Using this terminal, consisting of their terminal module - computer + reader - coupled to their card, a user can perform electronic transactions (electronic shopping, for example).

Of course, access of users to a terminal of this kind generates potential security risks.

The more decentralised the applications the greater the risk. Conversely, the better the control of the risks at the terminal end, the more decentralised can the applications be. Consider purse type applications, for example, in which transactions (purchaser card debit/merchant card credit) are effected card-to-card, without requiring consolidation of the transactions at the level of a centralised server.

It follows from the foregoing discussion that a terminal can potentially contain a set of information (or even software) on whose confidentiality and integrity the security of the application relies. Consider, for example, secret keys used to authenticate the terminal modules vis à vis the card or to encipher data transferred between a server and the card reader terminal module. An abuser with access to the terminal can analyse its operation and obtain access to the confidential information and software.

Note also that the applications referred to here, such as electronic shopping and electronic mail, are usually performed via the Internet. Experts are well aware that a personal computer (PC) connected to the Internet is highly vulnerable to viruses which can be installed and execute on the user's PC without them knowing it and without them allowing physical access to their computer to anyone at all. The totally invisible nature of this type of threat is the real danger currently limiting the deployment of transaction-based applications using the Internet. The same comments apply to electronic shopping applications on cable TV networks using set-top boxes connected to the TV set and incorporating one or two smart card readers.

The system level risks are then:

- Attack on the integrity of the cryptographic service provider and the application service provider with the aim of modifying the behaviour of the terminal module: for example, the terminal module is modified to capture information associated with the card and to store the information obtained for subsequent communication to a counterfeit server. This attack can be carried out unknown to the legitimate user (substitution of the user's terminal module or loan of a modified terminal module). This attack can then be generalised by circulating counterfeit terminal modules.

- Attack on the confidentiality of the cryptographic service provider, with the aim of

obtaining the cryptographic keys they use, which are stored on the hard disk of a computer, for example.

• Attack on other cards, based on the ability to authenticate the abuse vis à vis other cards by virtue of the secrets discovered by attacking the confidentiality of the service provider.

• Attack on the integrity and the confidentiality of communications between the various entities (application service providers, cryptographic service providers, integrated circuit card reader, integrated circuit card, server) to break the chain of confidence established between these elements. For example:

1 - deciphering communications between server and terminals;

2 - inserting third party software between the application service provider and the cryptographic service provider to break the chain of confidence between these two programs or to substitute for the application software third party software causing the security service provider to execute security requests with a different aim to that of the application known to the user.

• Attack on servers (in the case of an on-line application): connection of a counterfeit terminal to a server, emulation of a terminal module/integrated circuit card combination to obtain advantages.

An attack on the chain of confidence between the cryptographic service provider and the application service provider in the context of an application requiring an electronic transaction using an integrated circuit card to be signed is illustrated hereinafter. The transaction proceeds as follows:

- Step 1: verification of the personal confidential code (PIN) of the user, entered by the latter via a keypad associated with their terminal module, the code entered being sent to the card for verification by the latter.

- Step2 : authentication of the terminal module. The latter sends a "challenge request" command (a challenge is a random or pseudo-random number). The integrated circuit card generates the challenge and sends it to the terminal module. The terminal module sends the card an "external authentication" command accompanied by a response consisting of the challenge enciphered by a key held by the terminal module. The integrated circuit card then verifies the response received.

- Step 3: if steps 1 and 2 are executed satisfactorily, the integrated circuit card is ready to receive and to execute the signature command, i.e. command of encipherment, using a secret key stored on the card, of the result of a hashing operation performed on the transaction entered

by the user. After this encipherment the card sends to the terminal module the signature consisting of the result of the hashing operation enciphered in this way.

If the integrity of the application software (application service provider and its cryptographic service provider) is not assured, a hacker does not need to know the secret code and keys to pirate the transaction system; all that is necessary is to implant in the terminal module, for example the personal computer to which an integrated circuit card reader is connected, virus type software which in step 3 diverts the authentic data to be signed and sends falsified data to the card. Given that steps 1 and 2 have been executed in a satisfactory manner, the card will then sign the falsified data on the basis of the PIN that the user has entered and the user will believe that the card is about to sign their own data.

The preceding example shows the necessity of protecting not only the confidential information used in the context of a transaction but also the integrity of the transaction, i.e. the integrity of the behaviour of each entity involved in the transaction, together with the integrity of the behaviour of all of the software, assuring that the chain of confidence established between the various entities is broken.

The risks of attack mentioned hereinabove are currently covered in part by terminals - integrated circuit card readers integrating security modules (SAM, similar to an integrated circuit card) used in the context of purse applications in particular. The reader is then personalised by a SAM and assigned to a merchant, the cards read being those of customers. The SAM contains secret information and is able to execute algorithms using the secret information. However, it does not contain means for controlling communication with the user, with the integrated circuit card and/or with external electronic means, and for this reason the security of transactions is not assured.

Document WO 95/04328 discloses a terminal module comprising user interface means and interface means to external electronic means (hereinafter called external interface means) including an interface with a microcircuit card. The microprocessor of the terminal module comprises data storage means (ROM, EEPROM, RAM). The data stored in permanent memory (ROM) includes an operating system, managers of external components controlling the interfaces and peripheral devices, and an interpreter capable of interpreting program modules written in a specific language. The program modules are stored in the semi-permanent memory EEPROM and can be loaded into temporary memory RAM to be executed by the microprocessor on activation of an appropriate interface by the user. The program modules corresponding to the applications of the terminal module are downloaded into the EEPROM of the microprocessor or

into a microcircuit card from an external server.

The terminal module of document WO 95/04328 can operate:

- in autonomous terminal module mode, the microprocessor of the terminal module executing a program module stored in an internal memory without calling on an integrated circuit card;

- in autonomous terminal mode, in which a program module stored on a card is executed;

- in extended terminal mode or on-line mode, in which the microprocessor of the terminal module or that of the card executes a program module and communication is established via the telephone, a modem or a direct connection to a service provider or a server; and

- in transparent memory card reader mode, in which instructions received over a serial link are sent directly to the card and vice versa.

The terminal described in document WO 95/04328 does not deal with security problems addressed by the invention in that there is no description of how to secure a transaction to guarantee the integrity of the behaviour of all of the software executing the transaction. In particular there is no description of means for executing high-level requests issued by the application or how to guarantee the source, the integrity and the confidentiality of such means.

The present invention aims to provide a terminal for carrying out secure electronic transactions of the type comprising a personal security device such as an integrated circuit card or other device fulfilling the same functions and a terminal module provided with means of interfacing the personal security device, such as an integrated circuit card reader, and offering by virtue of its software and/or hardware architecture and the security mechanisms that it includes an enhanced level of security compatible with the fact that the terminal can be under the control of users (as opposed to terminals under the control of the operators).

A second objective of the invention is to assure this same level of security whilst enabling integration, during use, of new functions or applications, or modification of existing functions or applications without having recourse to a multitude of different terminal modules and without changing terminal modules to effect such modifications.

To this end, the invention consists in a terminal for execution of secure electronic transactions by a user in conjunction with at least one application installed on an electronic unit, said terminal comprising:

- a terminal module including at least:

* first interface means with said application for receiving from it requests relating to said transactions,

* second interface means with said user;

* third interface means with a personal security device,

* first data processing means comprising at least first software means for controlling said interface means, and

- a personal security device including at least second secure data processing means comprising at least second software means for executing elementary commands and means for executing cryptographic computations,

characterised in that:

- said terminal is adapted to receive said requests from said application installed on said electronic unit in the form of high-level requests independent of said personal security device,

- at least one of said terminal module and said personal security device comprises:

* at least one programmable memory for storing at least one filter program for translating said high-level requests into at least one of either (i) at least one command or a sequence of elementary commands for being executed by said second software means of said second data processing means, or (ii) at least one sequence of data exchanges between said terminal module and said user via said second interface means, said data exchanges being executed by said first software means of said first data processing means,

* means for protecting said filter software to prevent an unauthorised person reading and/or modifying said software, and

- at least one of said first and said second data processing means comprise a data processing device for executing said filter program.

The invention defined hereinabove achieves the security objectives required for carrying out electronic transactions by virtue of the fact that it describes a filter or "firewall" between the external world, i.e. the applications themselves, and the security means and peripheral devices that it controls, by means of a logical interface defining the format of high-level requests issued by the applications and of a translation software for processing these requests.

The terminal of the invention preferably comprises one or more of the following features, possibly in combination:

- said device for executing the filter program comprises first means for identifying and/or authenticating said application installed on said unit or the source of said requests sent by said application,

- said data processing device for executing said filter program comprises means for verifying the integrity of data received from said application,

- said data processing device for executing said filter program comprises centralised means for controlling conditions of use of services of the personal security device in accordance with said application and/or the user,

- said data processing device for executing said filter program comprises:

* means for commanding secured loading of said filter program into said programmable memory via said first or said third interface means from an entity external to said module, and

* first access control means for authorising said loading of said filter program only in response to at least one predefined condition,

- the terminal comprises second means for authentication of said first data processing means by said second data processing means,

- the terminal comprises third means for authentication of said second data processing means by said first data processing means,

- the terminal comprises a first communication channel between said first data processing means and said second data processing means and first means for securing said first communication channel,

- the terminal comprises fourth means for authentication of said terminal module by said user, independently of said card,

- said fourth authentication means comprise means for calculation by said first data processing means and for presentation to said user via said second interface means of a password known to said user and computed on the basis of a first secret parameter stored in said first data processing means,

- the terminal comprises fifth means for conjoint authentication of said terminal module and said card by said user, and

- said fifth authentication means comprise means for computation by said device for executing said filter program and for presentation to said user via said second interface means of a password known to said use and computed on the basis of at least second and third secret parameters stored respectively in said first data processing means and said second data

processing means.

In a first embodiment of the invention the terminal module is a personal computer and said programmable memory is the hard disk of said computer, said filter software is executed on the personal computer, or in a second mode of execution said programmable memory is on a secure server connected to the personal computer, the part of the filter software to be protected being executed on said secure server.

In a second embodiment of the invention the terminal module is a device such as a dedicated integrated circuit card reader, in which case said personal security device is an integrated circuit card or a personal computer. This embodiment differs from the preceding one in that said programmable memory is integrated into a secure microprocessor, said filter software being executed in said secure microprocessor. The dedicated terminal module can be portable.

Depending on the mode of execution of this second embodiment of the invention, the programmable memory for loading and storing the filter software can be in the personal security device or in the terminal module. In the latter case:

- the terminal module can include a single microprocessor for executing the filter software and for controlling the interfaces or two microprocessors respectively implementing these two functions ;

- preferably, said filter program comprises at least one secret parameter, and said second data processing means comprise second means of conditional access control for authorising execution of said cryptographic computations in response to elementary commands generated by said filter program only if at least a second predefined condition depending on said secret parameter is satisfied.

According to other features of the invention, when the terminal module comprises two microprocessors for executing the filter software and for controlling the interfaces :

- the terminal comprises a second communication channel between said first software means for controlling the interface means and said microprocessor and second means for securing said second communication channel ;

- said second securing means comprise means for encryption and decryption, by said first software means for controlling the interface means and said second microprocessor, of data sent on said second communication channel on the basis of at least a fifth secret parameter stored in memory on said storage means ;

- said second securing means comprise first physical means for protecting said second communication channel against intrusion.

Various embodiments of the invention will now be described with reference to the accompanying drawings, in particular embodiments in which the filter software is loaded and executed in the terminal to guarantee its source, its confidentiality and its integrity, the software being also able to authenticate the source of requests sent to it if confidence in the interfaces with the user, i.e. the screen and the keyboard, cannot be guaranteed.

- Figure 1 is a diagram showing the functional architecture of a system for carrying out secure transactions by means of a terminal in accordance with the invention;

- Figure 2A shows a first embodiment of the invention in which the terminal is a personal computer connected to an integrated circuit card by a reader, the application being installed on the personal computer or on a remote server;

- Figure 2B explains the functional architecture of one variant of the first embodiment of the invention in which the personal computer serving as a terminal is connected to a security server on which the filter software is installed;

- Figure 3 shows a transaction system using a terminal constituting a second embodiment of the invention, which can be a dedicated product connected as a peripheral device to a personal computer or directly to a server or based on a personal computer;

- Figure 4A is a block diagram of the hardware architecture of the electronic circuits of a first mode of execution of the terminal from figure 3;

- Figure 4B is a functional diagram illustrating a first software architecture configuration of the terminal from figure 4A;

- Figure 4C is a functional diagram similar to that of figure 4B showing a second software architecture configuration of the terminal from figure 4A;

- Figure 5 is a block diagram of the hardware architecture of the electronic circuits of a second mode of execution of the autonomous terminal from figure 3;

- Figure 6 is a block diagram of the hardware architecture of the electronic circuits of a third mode of execution of the autonomous terminal from figure 3;

- Figure 7 is a diagram illustrating the conventional software architecture of a microcircuit card;

- Figure 8A is a diagram illustrating the software architecture of a transaction system comprising the terminal from figure 4A;

- Figure 8B is a diagram illustrating the software architecture of a transaction system comprising the terminal from figure 6;

- Figure 9 is a diagram illustrating the implementation of an electronic trading

application by means of a system in accordance with the invention; and

- Figure 10 is a flowchart showing the process of downloading a program into a reprogrammable memory of the terminal module from figure 4A or figure 5 or of a microcircuit card connected to the latter.

Referring to figure 1, a system for carrying out secure transactions comprises a terminal module 1 for reading an integrated circuit card 31 or the like. The terminal module 1 comprises a filter F consisting of a software module processing high-level requests issued by application service providers FAp external to the terminal module 1 by means of a logic interface F-API and user interfaces such as a display screen 4 and a keyboard 5 enabling a user to read and enter data. It also comprises a reader or other communication interface 6 with a microcircuit card or any equivalent security device personal to the user of the token, "Java Ring" (from SUN), "iButton" (from Dallas Semiconductor Corporation), or soft token type and communication interfaces with at least one application service provider FAp which can be installed on a PC and/or on a server Sap, for example, data then being exchanged via a data communication or telecommunication network R.

The terminal module 1 can be a dedicated terminal or integrated into a PC or into a network computer (NC) dedicated to network applications or into a cable TV network decoder (Set Top Box).

The terminal module 1 can perhaps be used in autonomous mode, for example to read information such as the contents of an electronic purse contained in a memory of the card 31.

To carry out secure transactions the terminal module 1 can be used on-line to a server Sap or off-line, the application FAp then running locally, for example on the PC: this is the case when, for example, a user must sign an electronic mail message or transactions that will be sent to an addressee. An operation of this kind does not imply connection to an application server at the time when the card 31 is used.

In on-line mode, as represented in figure 3 in the case of a dedicated terminal module 1, the latter can be connected to the server Sap on which the application FAp is installed via the PC and a network R such as the Internet or through the intermediary of the telephone network R via a modem MO or a DTMF link with a telephone handset CT. Some transactions, such as reloading an electronic purse in the card 31, can necessitate bidirectional exchange of data with the server Sap and are therefore more ergonomic in on-line mode.

Carrying out a transaction secured with a terminal module 1 and a card 31 implies that high-level software requests (for example: requests for signature, authentication, etc... which

must be processed so as to meet the required security objectives of the application program) will be sent from the application program installed on the server Sap for example (on-line mode) or in the PC or NC available to the user (off-line mode, for example signing of electronic mail) to the filter F controlling the security means. The filter F processes these requests by means of translation software to assure that the application or virus type software cannot have direct access to the cryptographic functions of the integrated circuit card 31. The processing of the high-level requests includes translation of these requests into an elementary command or a sequence of elementary commands which are executed by the personal security device. The high-level requests are formulated independently of the software and/or hardware design of the personal security device, i.e. they are not formulated as a direct function of the personal security device.

The high level requests contain information specifically related to the process that will be executed by the filter F. In a simple example, a high level request can contain a single elementary command to be transferred to the personal security device, for example, an APDU (Application Protocol Data Unit) in the case of a smart card, attached to a Message Authentication Code that will enable the filter F to check the origin and integrity of this request before sending the elementary command to the personal security device. In a more complex example such as a request to sign a document, the high level request will be transformed by the filter F into a sequence of elementary commands sent to the personal security device and eventually to the user interface. Thus, according to this definition and due to the fact that it contains specific information to be decoded by the filter F independently of the personal security device, the high level requests will be said to be independent of the personal security device.

The filter F meets the security objectives required in that the translation software that it includes verifies the identity of the application issuing the service requests (or the source of requests directly) and is installed in a manner that guarantees the integrity and the confidentiality of the operations and data used to respond to service requests.

A translation software is configured for one type of microcircuit card and translates a high-level request received from application software into an elementary command or a sequence of elementary commands that can be executed by the microcircuit cards and/or a sequence of exchanges of data with the user.

The high-level requests are a list of commands used by the application programs to invoke the security services needed to identify and authenticate the person performing the transaction and to guarantee the source, the integrity and where applicable non-repudiation of

the transaction. A high-level request from an application (on a server or on the PC or NC) can be characterised by one or more of the following points :

- it is independent of the basic means (cryptographic means, for example) used to respond to its request and contains specific information to be processed by the filter F. Reciprocally, a plurality of applications can use the same security service provider, employing the same logic interface F-API defining these requests.

- the processing of the request links the transaction in a certain manner to the user performing the transaction by means of at least one fixed or variable secret parameter stored in by the integrated circuit card of the user.

- it can include information enabling the filter software F to verify its source and its integrity. Authentication can use a Message Authentication Code (MAC) or a code of the electronic signature type associated with the request.

- if the transaction is not entered by the user on the terminal module itself, the request can contain the information needed for the user to verify the essential data of the transaction, if required and if the terminal module supports this option.

The logic interface F-API for exchanging high-level security requests between the application and the translation software of the filter F can be standardised so that it is common to different application programs. Accordingly, the signature type request can be used by an electronic mail application and by purchasing software. It is therefore possible to change the application whilst retaining the security service provider or vice versa to replace the security service provider without changing the application.

To guarantee the integrity of the chain of confidence between the application and the card, the translation filter software F identifies and even authenticates the source and the integrity of requests that it receives. Various methods are feasible for identifying the application issuing the requests:

- an identification code can be integrated into the request itself and then verified by the filter software using information that it contains or that can be stored on the integrated circuit card;

- the same objective can be achieved by comparing the result of a hashing operation executed by the filter software on the application software issuing the request with a result previously stored on the card, for example. This solution is particularly suitable for the situation in which the application is installed on the user's PC;

- authentication can equally be performed by associating with the request a MAC

calculated from the content of the request and a secret key shared between the application and the filter software. An equivalent principle can be used with a signature on the request calculated with the same information and a private key known to the application, the signature being verified with the corresponding public key known to the filter software.

Figure 2A explains a first embodiment in which the terminal module 1 is a PC 102, the connection to the integrated circuit card 31 employing a reader 6 connected to or integrated into the PC 102. The PC 102 includes input/output interfaces 102a to the reader 6 and the server Sap. Depending on the nature of the reader connected to the PC, the user interface components can be the keyboard and the screen of the PC itself or a keyboard and/or an LCD display on the reader, for example. In this embodiment the filter F is installed and executes on the PC 102. The filter F, and therefore the translation software that it contains, can be stored on the hard disk (HD) 102b of the personal computer 102. To execute on the central processor unit or microprocessor 102c of the PC, the filter software is loaded into the random access memory (RAM) 102d of the personal computer 102.

Because the hard disk of a PC is difficult to protect, the filter software F or at least the sensitive part of this software can be encrypted. For this purpose it can be divided into at least two modules: a loading/decrypting module Fcd and a second module corresponding to the encrypted filter software itself. The first module enables the second module to be loaded into RAM, decrypted and then executed. Referring to figure 2A, the software module when decrypted and loaded into RAM is denoted Fdec.

Programming languages like Java, with security mechanisms intrinsic to the language itself, strengthen the protection of the software.

Another method of verifying the integrity of the filter software is to have the second module signed by an authority guaranteeing the content of the filter software by means of a private key that is kept secret by the authority. The first loading module then, at the same time as performing the decrypting operation, performs a hashing operation on the second module and verifies the signature of this module using the public key associated with the private key of the authority.

The operations described above imply the use of keys on which the security of the application relies. These keys can be concealed in the loading module, stored in the reader 6, or stored on the integrated circuit card 31 itself. Another possibility is to install the decryption and integrity verification module in the reader 6.

The object of the invention is to prevent a pirate from using the integrated circuit card of

a user without their knowledge, for example by modifying the filter software controlling the card or the application software, or by loading a virus to bypass the application or the filter software. The embodiment described previously and its variants address these risks, by enabling verification of:

- the integrity of the filter software, and

- the source and the integrity of commands sent to the card via the reader 6, by authenticating them using a MAC, for example. The MAC can be verified by the reader 6 or the card 31. Equivalent protection could be obtained by encrypting the dialogue between the filter software and the reader 6. A virus attempting to bypass the filter software would then send unauthenticated or incorrectly encrypted commands to the reader 6 or to the card 31; these commands would therefore be rejected by the reader or the card, preventing the virus from achieving its aims. To prevent a hacker from determining the keys used by a terminal by analysing the operation of another terminal, the keys used by various terminals must be diversified.

The encryption and signature mechanisms that can be considered to address the need to protect the filter software are well known to the skilled person and are based on existing cryptographic techniques as described, for example, in "Applied Cryptography, Protocols, Algorithms, and Source Code in C" by Bruce Schneier, John Wiley and Sons, Inc., 1994 and for this reason will not be described in detail here.

Installing the filter software on a PC cannot guarantee the same level of security as installing it in a dedicated terminal that can offer additional hardware security mechanisms as used in the other embodiments described later, these mechanisms offering physical protection of the filter software and the secrets that it contains.

Figure 2B shows one variant of the figure 2A embodiment. This variant exploits the flexibility and the ease of connection of a personal computer to a network. This enables part of the filter software, and in particular the secrets, to be held by a secure server Ssec.

In figure 2B the filter software is divided into two software modules, a module F-PC installed on the PC 102 and a module F-SE installed on a security server Ssec. The programmable memory previously referred to and storing the filter software is therefore in the secure sever Ssec in this variant, i.e. out of reach of unauthorised users. Likewise, the filter software or at least the sensitive part of the filter software F-SE requiring protection executes on the secure server Ssec.

The software module F-PC installed on the PC 102 is connected by a secure channel

CS to the security server Ssec. The secure channel is an encrypted communication channel for exchanging protected data between the two filter software modules F-PC and F-SE and possibly reciprocal authentication of the two modules F-PC and F-SE. The secure channel can use well-known communication protocols such as SSL, for example.

Setting up this secure channel CS therefore enables the first filter software module F-PC to send to the second filter software module F-SE requests received from the application FAp via the logic interface F-API together with information concerning identification of the application issuing these requests. After verifying the information relating to the application, and depending on the application and possibly on rights of the user, the second software module F-SE then translates these requests into a series of commands to the microchip card 31 and for controlling exchanges of data with the user. The commands generated by the module F-SE are then sent to the first module F-PC which routes them to the element concerned: the PC itself in the case of the commands controlling exchanges with the user or the integrated circuit card. For the commands controlling exchanges with the user to execute on the PC, the latter must include an interpreter software module I. The interpreter software enables display of messages on the screen 4 and input of information by the user via the keyboard 5. The interpreter software module is described in more detail in connection with figures 4B and 4C.

This second mode of execution is based on the mechanisms described à propos the first mode of execution (figure 2A) insofar as the identification of the application (hashing or signature, for example) and protection of commands sent to the card (addition of a MAC, for example) are concerned. On the other hand, it offers an enhanced degree of security insofar as the filter software module F-SE translating high-level requests received from the application FAp executes in a secure environment. In the context of the invention the server Ssec is deemed to be secure if it is not accessible physically or logically (i.e. via a network connection) to unauthorised persons.

The second mode of execution shown in figure 2B is suitable for applications employed in a closed or private environment controlled by a central authority, as it necessitates a protected server administered centrally. This second mode of execution also offers the facility to define a centralised policy of access to cryptographic services offered by the integrated circuit card. This access policy can be based on applications requiring the services of the card and on the users themselves. In the case of a business issuing its employees or customers integrated circuit cards enabling them to sign electronic mail and banking transactions, it can assure that only authorised users can sign: this mechanism can be implemented using the secure channel CS.

For each signature request issued by one of the applications deemed to be valid by the business (the electronic mail program and the bank transaction software), the software module F-SE will execute a request for authentication of the user. This request can be executed, for example, by sending a random number (challenge) to the card 31 via the secure channel CS. After the user enters their confidential code, the integrated circuit card calculates a dynamic password by encrypting the challenge using a secret key that it holds. The password is then sent via the secure channel CS to the software module F-SE. Knowing the user and therefore the secret key held on their card, the software module F-SE compares the password received with the password expected. This mechanism, known as challenge-response mode authentication, enables the software module F-SE to validate the user's identity. Thus the business that has issued the integrated circuit cards to the users can assure that only users who are still authorised can sign bank transactions, for example.

By virtue of the secure and centralised means that it represents, the server Ssec enables not only secure installation of the filter software F-SE but also the facility of instituting a centralised policy for controlling use of security services offered by the integrated circuit card. The server Ssec enables a centralised policy to be instituted by virtue of the fact that the same server can be connected to a plurality of software modules F-PC installed on the personal computers of a plurality of users. Thus the server Ssec enables centralised definition and control of the conditions of use of security services offered by the cards issued to the various users in accordance with the profile of the application requesting the services and the rights of said users. Instituting this centralised policy implies the server holding the necessary information, i.e. the rights of users to use a particular security service in connection with a particular application.

This second mode of execution (figure 2B), well suited to private environments, is difficult to apply to open applications where a secure central server Ssec is not feasible.

Figure 3 shows a terminal module embodying functional architecture principles similar to those of figure 2B in a different embodiment requiring no centralised server. The terminal module in the second embodiment of figure 3 has a very high level of security, enabling it to assure local protection of the filter software F directly.

In figure 3 one face of the terminal module 1 which can be a portable unit, carries the display screen 4 and the keyboard 5 and the unit contains the electronic circuits, which are preferably not accessible from the outside. The module 1 contains the reader 6 and has an opening for inserting the microcircuit card 31 into the reader 6. The mode of execution described with reference to figures 3, 4A, 4B and 4C must not be considered as limited to a dedicated

terminal. The following description applies to a PC-based or NC-based terminal.

In a first mode of execution, shown in figure 4A, of this second embodiment of the terminal module of figure 3, the electronic circuits of the terminal module 1 are based on a standard microcontroller 2 and a secure microprocessor 3 which are interconnected and permanently installed in the module 1. As an alternative to this, the microprocessor 3 can plug into the module 1 by means of a connector 41 shown in dashed line in figure 4A. This description covers a generic mode of execution based on a standard microcontroller. In a particular mode of execution that will be described later the microcontroller 2 can be a PC 102 of the type shown in figure 2B.

The standard microcontroller 2 comprises a processor unit 2a, temporary memory (RAM) 2b and permanent memory (ROM) 2c. It is preferably a "monochip" microprocessor the software of which is mask-programmed in the permanent memory 2c and which integrates into the same integrated circuit standard interface management or control means, the processor unit 2a, the temporary memory 2b and the permanent memory 2c.

The interfaces or peripheral devices managed by the microcontroller 2 include the data display screen 4, for example a liquid crystal display, the keyboard 5 for entry of data by a user, the microcircuit card reader 6, an external connection interface 7, for example of the RS 232 or PCM-CIA type, an infrared link interface 8 and a DTMF device 9 for sending data over a telephone line.

The components of the module 1 also include a clock 10 and an electrical power supply 11 for the various circuits and components of the module 1. The electrical power supply 11 can be a battery power supply if the module 1 is portable and autonomous.

The task of the standard microcontroller 2 is to manage the environment, i.e. to control the interfaces 4-9 and the clock 10 together with the power supply 11 for selectively energising the secure microprocessor 3 in the case of an autonomous module 1.

The standard microcontroller 2 therefore requires little computing power, little temporary memory (RAM) and no semi-permanent memory (EPROM OR EEPROM). The microcontroller 2 is write protected by virtue of the fact that programs (interface control and, as described below, interpretation, management of clocks and electrical power supply, etc) are mask-programmed in the permanent memory 2c. As will become apparent hereinafter, the standard microcontroller 2 can also contain one or more secret parameters on the basis of which it can be authenticated by the secure microprocessor of the terminal module and/or of an integrated circuit card. The secrets must therefore be protected against reading and writing.

They are preferably stored in the temporary memory (RAM) of a "monochip" microprocessor which cannot be written or read from the outside. The standard microcontroller 2 can also have additional security functions, for example to prevent fraud such as display of data different to that coming from the microprocessor 3.

It is therefore of low cost and consumes little electrical power, which is particularly suitable for a portable product. The microcontroller can be an OKI MSM 63180, for example.

There are preferably two clocks 10: a low-frequency clock 10a, for example a 32.368 kHz clock, and a high-frequency clock 10b, for example a clock at 1 MHz to 12 MHz. The microcontroller 2 commands the connection of its system clock to one or other of these two clocks.

The slow clock 10a times a timer 2d of the microcontroller 2 with a period of 0.5 s to provide a real time clock in the module 1. The processor unit 2a can also use the slow clock 10a for functions that do not require high calculation speed: in this case the system clock of the microcontroller 2 is connected to the slow clock 10a and the fast clock 10b is stopped. This mode of operation reduces the electrical power consumption of the module 1 which is advantageous if it is portable and battery powered.

The microprocessor 3 which is read and write protected includes a central processor unit 3a, a temporary memory (RAM) 3b and a permanent memory (ROM) 3c, together with electrically reprogrammable semi-permanent memory (EEPROM or Flash RAM, for example) 3d for storing the application programs of the module 1.

The secure microprocessor 3 is of the type used in microcircuit cards and has a limited number of inputs and outputs, its internal buses being inaccessible from the outside. It is manufactured with other security mechanisms specific to this type of microprocessor and well known to the skilled person, such as security matrix, memory scrambling, clock frequency control, reset control, etc mechanisms.

Because the microprocessor 3 has a semi-permanent memory 3d it is possible to load one or more application programs into it from the outside, for example from a server or from a microcircuit card. It is therefore possible to modify the application(s) in accordance with requirements (access control, financial and/or commercial transactions, electronic purse, etc) for which the module 1 is intended. If the size of the semi-permanent memory 3d allows it, it is also possible to install new applications during its use.

Depending on the version chosen, the secure microprocessor 3 can compute cryptographic functions requiring large-scale computations embodied in RSA or DSA type

asymmetric algorithms or use simpler algorithms, for example DES type algorithms.

The secure microprocessor 3 can be, for example:

- a SIEMENS SLE44C160S non-cryptographic micro-processor, with 14 kbytes of ROM and 16 kbytes of EEPROM;

- an SGS THOMSON ST16CF54A cryptographic micro-processor, with 16 kbytes of ROM, 4 kbytes of EEPROM and 480 bytes of RAM;

- a PHILIPS P83C858 cryptographic microprocessor with 20 kbytes of ROM and 8 kbytes of EEPROM.

The secure microprocessor 3 is connected by the link 12 to the standard microcontroller 2 and by links 13 and 14 to the external interface 7 and to the microcircuit card reader 6 via respective switches-interface adapters 15 and 16. The switches-interface adapters 15 and 16 are controlled by the standard microcontroller 2 via respective links 17 and 18.

The standard microcontroller 2 comprises an interpreter program 20 (figs 4B and 4C) stored in the ROM 2c and enabling it to execute commands generated by the software for translating high-level requests forming part of the application or program(s), as described hereinafter. The interpreter 20 enables application programs stored in the secure microprocessor 3 to control the interfaces 4-9 via the link 12. The application programs can nevertheless be located and executed elsewhere than in the secure microprocessor 3, for example on a microcircuit card 31 inserted into the interface 6, for example a card supporting mechanisms for downloading and executing applications as described in French Standard NF EN 726-3, the title of which translates as "Integrated circuit cards and terminals for telecommunications. Part 3: Specifications of the card independent of the applications".

Depending on the security rules to which they are subject, the application programs can also be divided between these various locations.

Figure 4B is a functional diagram showing a first software architecture configuration of the module 1 from figure 4A in which all application programs A1, A2, ..., An and security functions (condensate computations, symmetrical cryptographic algorithms such as DES or triple DES, asymmetric cryptographic algorithms as proposed by RSA) are implemented in the secure microprocessor 3.

The applications denoted A1, A2, ..., An hereinabove and in the remainder of the description comprise at least the filters F1, F2, ..., Fn and thus in particular the software for translating requests from the application service provider(s) FAp forming part of the main application 54 (figure 8A).

The standard microcontroller 2 manages the environment using various interface drivers:

- a driver 21 for the microcircuit card reader or interface 6;
- a driver 22 for the serial link interface 7;
- a driver 23 for the keyboard 5;
- a driver 24 for the infrared link interface 8;
- a driver 25 for the display 4;
- a driver 26 for the clock 10 and the power supply 11;
- a driver 27 for the DTMF interface 9; and
- a driver 28 for other interfaces, assuming that the module 1 includes one or more interfaces other than those represented in figure 2.

The secure microprocessor 3 can therefore control the interfaces by means of commands which are interpreted by the interpreter 20 and executed by the standard microcontroller 2 using the drivers 21-28.

Figure 4C shows a second software configuration of the module 1 from figure 4A in which one or more applications Ax and one or more cryptographic functions Sx are stored in a reprogrammable memory 30a of a secure microprocessor 30 of a microprocessor card 31. When the card 31 is inserted into the reader 6, the microprocessor 30 executes the applications Ax and the cryptographic functions Sx. Other applications and security functions can be resident in and executed by the secure microprocessor 3 of the module 1. For example, the microprocessor 30 of the card 31 can assure an electronic signature function assuming that the secure microprocessor 3 does not include a dedicated computation processor (cryptoprocessor). Reciprocally, if the secure microprocessor 3 includes a cryptoprocessor, it is possible for an application on the microcircuit card 31 to invoke cryptographic commands of the module 1 that will be executed by the secure microprocessor 3.

In this second configuration, which otherwise is identical to that of figure 4B, the interpreter 20 has the same role relative to the microprocessor 30 as it has relative to the secure microprocessor 3. Thus the module 1 can execute different applications according to the type of microcircuit card 31 inserted into the reader 6, for example:

- authentication of the user in the context of a banking transaction (balance enquiry, transfer of funds, etc) effected via a telephone line by means of the DTMF interface 9;
- electronic purse balance enquiry or reloading from the module 1 when a microcircuit card 31 used as a purse is inserted into the reader 6. The module 1 offers the facility to manage

several different purses: bank purse, purse specific to an institution, for example;

- reading a medical dossier on a medical card;

- reading loyalty points on a card on which loyalty points are awarded to a consumer according to purchases made, participation in customer loyalty operation, etc.

The mode of execution described hereinabove with reference to figure 4A and the software configurations shown in figures 4B and 4C likewise apply to a terminal based on a conventional PC additionally equipped with a secure microprocessor 3. In this mode of execution the microcontroller 2 corresponds to the PC 102 as shown in figure 2A, the processor unit 2a corresponds to the microprocessor 102c of the PC and the RAM 2b and the permanent memory 2c respectively correspond to the RAM 102d and the hard disk 102b. Likewise the inputs/outputs 102a of the PC correspond to the interface modules 7, 8 and 12 of figure 4A. The connection between the secure microprocessor 3 and the PC 102 can be a serial or parallel link or a connection to the PCMCIA type internal bus of the PC, or a direct connection to the PC motherboard. As an alternative to this, the secure microprocessor 3 can be fixedly or removably (via the connector 41) integrated with the PC keyboard.

In this case the interpreter software module 20 and the peripheral driver software modules 21 through 28 are installed on and executed on the PC. The functional architecture of this mode of execution is equivalent to that shown in figure 2B, the interpreter module 20 installed on the PC assuring the same role as the interpreter module I from figure 2B: it executes commands for controlling exchanges with the user received from the filter software F which is installed in a secure manner in the microprocessor 3 (Figure 4B) or the integrated circuit card 30 (Figure 4C).

The figure 5 diagram illustrates a second mode of execution of a second embodiment of the invention in which the electronic circuits of the terminal module 1 are based on a single microcontroller 29 replacing the microcontroller 2 and the microprocessor 3 and offering the same type of physical and logical protection as the microprocessors designed for integrated circuit cards. This microcontroller drives all the interface means 4-9 of the terminal module. It includes a processor unit 29a, a temporary memory (RAM) 29b, a permanent memory (ROM) 29c and a semi-permanent memory (EEPROM) 29d for storing the translation software. The processor unit 29a corresponds to both the data processing unit 2a controlling the interfaces and the processor unit 3a for executing the translation software. As previously, the terminal module 1 can be based on a PC 102 to the internal bus of which is connected a secure microcontroller 29 controlling the display screen 4 and the keyboard 5 of the PC directly.

In one variant the memory in which the software for translating high-level requests is stored, volatile RAM with backup power supply or semi-permanent memory (EEPROM or Flash RAM), can be external to the microcontroller 29. In this case the translation software can be encrypted and signed or protected by a message authentication code (MAC) to assure its integrity and it confidentiality. The software is read by the microcontroller 29, decrypted and then executed.

In a third mode of execution represented in figure 6 of the second embodiment of the invention the terminal module 101 has no secure microprocessor 3. In figure 6 the same reference numbers as in figure 4A denote the same elements. The microcontroller 2 controls the interface 6 and the switch-adapter 15 for connecting the secure microprocessor 130 of a programmable microcircuit card 131 in the interface 6 with the external link interface 7. In this case all of the applications A and the cryptographic functions C are stored in a semi-permanent memory (EEPROM or Flash RAM) 130a of the secure microprocessor 130 of the programmable microcircuit card 131 and implemented by the latter as described with reference to figure 4C in respect of the applications Ax and the cryptographic functions Cx.

In the examples described previously, for simplicity, the microprocessor 30, 130 of the integrated circuit card and the secure microprocessor 3 possibly incorporated in the terminal module have a single communication port. This implies that in these examples exchanges between the various entities, i.e. the electronic unit 154 (figure 8) containing the main application, the secure microprocessor 3 and the microprocessor 30, 130 of the integrated circuit card, are effected via the microcontroller 2 or 29 of the terminal module. The above descriptions must not be considered as limiting on the invention: other implementations are feasible within the scope of the present invention. The secure microprocessors for integrated circuit cards currently available which can be used for the card itself (microprocessor 30, 130) or in the terminal module (microprocessor 3) can have two communication ports. Various embodiments optimising communication are therefore easy to envisage with this type of microprocessor. In figure 4C, for example, one port of the integrated circuit card 31 can be dedicated to controlling the user interface and therefore connected to the microcontroller 2, the other port being connected to the electronic unit including the main application, subject to appropriate interface adaptation.

According to one important feature of the invention filter software is stored in the reprogrammable memory EEPROM associated with the secure microprocessor 3 or 29 of the terminal module 1 and/or the secure microprocessor 30, 130 of the card 31, 131. This filter software translates in a manner known in itself high-level requests from the server Sap or from

the PC into sequences of elementary commands that can be executed by these microprocessors (these commands are defined in part 4 of ISO standard 7816-4). In accordance with the invention, this filter software translates these high-level requests into sequences of exchanges of data between the terminal module 1, 101 and the user via the interface means such as the display 4 and the keyboard 5.

This solution has the advantage of considerably reducing the flow of data exchanged between the terminal module 1, 101 and the server Sap or the PC, but requires secure installation of the translation software to prevent instructions sent to the microcircuit card from being modified.

This filter software is an integral part of the portion of the application software installed in the terminal module 1 and/or the card 31, 131 and can therefore be downloaded.

Figure 7 illustrates the conventional software architecture of a microcircuit card (smart card).

The various software layers are represented by a block 43 which comprises a "communication protocol" software layer 44 enabling commands to be received. These commands are decoded by an "APDU command interpreter" software layer 45 (APDU: Application Protocol Data Unit) the role of which is to route the commands to the processing modules, which can be:

- secure file management services software 46;
- cryptographic services software 47;
- application software 48.

The processing modules 46, 47, 48 rely on basic services offered by the operating system 49 of the microcircuit card.

Figure 8A illustrates the software architecture of a system for carrying out secure transactions using terminal modules 1 provided with a secure microprocessor 3 in accordance with the mode of execution of the invention shown in figure 4A.

Block 51 represents the software executed by the secure microprocessor 3 of the terminal module 1, block 52 the software executed by the microcontroller 2 or the PC 102 of the terminal module 1, block 53 the software executed by the microprocessor 30 of a microcircuit card 31 and block 54 the main application software (application service provider) installed on the server Sap or on a PC.

Block 51 is similar to block 43 of figure 7, i.e. the secure microprocessor 3 has an architecture similar to that of an integrated circuit card. Block 51 comprises:

- communication protocol software 60;

- operating system 61;

- a block 62 representing the portion of the application software installed in the terminal module 1, this portion of the application software essentially comprising the filter software previously mentioned. Various software modules of this type corresponding to various applications can co-exist in the secure microprocessor 3;

- optionally, software 63 for authentication of the standard microcontroller 2 (by the secure microprocessor 3) and authentication of the secure microprocessor 3 of the terminal module 1 (by the microprocessor 30 of the card 31);

- secure file management software 64;

- cryptographic services software 65.

Block 52 comprises:

- communication protocol software 70;

- a command interpreter 71 corresponding to the software 20 from figures 4B and 4C;

- authentication software 72 for authentication of the standard microcontroller 2 (by the secure microprocessor 3 of the terminal module 1) in conjunction with the software 63;

- software 73 for controlling resources internal to the microcontroller 2;

- software 74 for controlling interfaces with the user drivers 23 and 25 for the screen 4 and the keyboard 5);

- software 75 for controlling the communication interfaces 7, 8 and 9 (drivers 22, 24, 27).

Finally, block 53 is similar to block 43 but in the example described with reference to figure 8A does not include any application or filter software. It comprises:

- communication protocol software 80;

- APDU command interpretation software 81;

- secure file management services (for example PIN checking) software 82;

- cryptographic services software 83 (symmetrical cryptographic computations using secret keys or asymmetric cryptographic computations using public and private keys, etc) for authentication of the secure microprocessor 3 of the terminal 1 (by the microprocessor 30 of the card 31) in conjunction with the software 63, among other functions;

- the operating system 84 of the microprocessor 30 on the card 31.

The communication protocol 60, 70, 80 controls exchange of data between:

- the microprocessor 30 of the card 31 and the standard microcontroller 2 of the

PC 102 of the terminal module 1;

- the secure microprocessor 3 and the microcontroller 2 of the terminal module 1;

- the secure microprocessor 3 of the terminal module 1 and the microprocessor 30 of the card 31.

Figure 8B is a view similar to figure 8A illustrating the software architecture of the system in the situation where the terminal module 101 does not include the secure microprocessor 3, in accordance with the third mode of execution of the second embodiment of the invention (figure 6).

In figure 8B, block 152 represents the software executed by the microcontroller 2 of the terminal module 101, block 153 the software executed by the microprocessor 130 of a programmable microcircuit card 131, and block 154 the main application software installed on the server Sap or on a PC.

Block 152 comprises the same software 70, 71 and 73 through 75 as block 52 from figure 8A and a block 76 which comprises software for authentication of the standard microcontroller 2 of the terminal module 101 (by the microprocessor 130 on the card 131).

Block 153 relating to the microprocessor 130 of the card 131 comprises software 62 and 80 through 84 of blocks 51 and 53 from figure 8A together with software 77 for authentication of the standard microcontroller 2 of the terminal module 101 (by the microprocessor 130 of the card 131) in conjunction with the software 76.

Unlike a conventional system, in a secured transaction system of the invention the filter software 62 which translates high-level requests from the application into elementary commands that can be executed by a microcircuit card is installed in the secure user environment, i.e. either in the terminal module 1 (for the applications A1, A2, ..., An of the modes of execution from figures 4A-4C and 5) or on a semi-permanent memory card 31, 131 which can be used with the terminal module 1, 101 (for the applications Ax of the figure 4C embodiment and for all the applications of the figure 6 embodiment).

Apart from its microcircuit card management function, the filter software 62 controls interaction with the user, i.e. the sequences of exchanges of data between a user and the terminal module which are required in the context of an application and which use the interface means, namely the screen 4 and the keyboard 5. Note that the invention is not limited to the use of a screen and a keyboard as interfaces with the user and that any other type of interface with the required ergonomic features could be suitable, for example a voice interface.

Transactions are secure because the filter software 62 is securely installed in the

secure microprocessor 3 or 29 of the terminal module 1 or the microprocessor 30, 130 of the microcircuit card 31, 131. The keys and rules necessary to access files on the microcircuit card 31, 131 are contained in the translation software 62 and are therefore inaccessible to third parties.

The functions of the filter software 62 will be illustrated hereinafter in the context of an example of an electronic trading application. The application includes the following entities:

- a purchaser,
- a merchant,
- a bank.

The merchant has an electronic trading server Sap (Web server) accessible via the Internet. The purchaser has:

- a PC for accessing the electronic server Sap to consult a catalogue of products,
- an integrated circuit card 31 supplied by the bank and the microprocessor 30 in which contains a private key but does not have any cryptographic capabilities connected with a signature,
- a terminal module 1 as shown in the figure 4A embodiment, having a standard microcontroller 2, a secure microprocessor 3 with cryptographic capabilities enabling a message to be signed, a keyboard 5, a display 4, an integrated circuit card interface 6 and a serial interface 7 for connecting it to a PC.

The principle of operation is as follows: the transaction is signed by the terminal module 1 using a private key held by the card 31. This private key is protected by a confidential code (PIN) that the purchaser must enter in a secure environment, i.e. on the terminal 1, and by prior authentication of the terminal 1 by the card 31 using a secret key Kauth. The private key is also transmitted in an encrypted manner (by means of a key Kchif) to set-up a secure communication channel between the microprocessor 30 of the integrated circuit card 31 and the secure microprocessor 3 of the terminal 1.

Figure 9 illustrates the exchanges between the various entities:

a. the purchaser enters an order on the PC,

b. the PC generates the transaction to be signed by the purchaser (product code, price) and requests the terminal module 1 to sign the transaction,

c. the terminal module verifies the source of the request for signature and then prompts the user to enter their PIN code by displaying a message "enter PIN" on the display 4,

d. the purchaser enters the code (PIN) on the keyboard 5 of the terminal module 1,

e. the terminal module 1 sends the PIN to the card 31 for verification; positive verification lifts one of two conditions of access to reading the private key,

f. the terminal module 1 displays the transaction on its display 4,

g. the purchaser confirms it by pressing a "confirm" key on the keyboard 5 of the terminal module 1,

h. the terminal module 1 submits an external authentication request to the card 31. External authentication enables the secure microprocessor 3 of the terminal module 1 to authenticate itself to the microprocessor 30 of the card 31 and thereby lift the second level of protection of access to the private key. This authentication is performed in challenge/response mode using a secret Kauth shared by the terminal module 1 and the card 31,

i. the terminal module 1 sends a private key read request to the card 31,

j. all access conditions having been satisfied, the card 31 accepts the read request and sends the private key, which is encrypted using a secret key Kchif shared by the card 31 and the terminal module 1,

k. the terminal module 1 decrypts the private key, signs the transaction by means of the private key, destroys the private key, disconnects from the card 31 and sends the signed transaction to the PC which sends it to the server S.

The above example can easily be transposed to an electronic transaction performed without any PC, the terminal module 1 being connected directly to a server Sap by a modem link (figure 3), the purchaser entering the order (product code) on the terminal module 1.

Note that authentication of the secure microprocessor 3 by the card can also be effected by way of the read private key command by associating with it a message authentication code (MAC) calculated using a secret key.

This example shows that the filter software 62 can translate a high-level "request for transaction signature" into a multitude of individual requests addressed to the various interfaces of the terminal interface 1, namely its interface 6 with the integrated circuit card 31, its interface with the display 4, its interface with the keyboard 5 and its interface for connecting it to the PC or the server Sap.

Translation filter software of this kind has a screening role, providing a filter between the outside world, i.e. the applications, and the peripheral devices that it controls.

It enhances security because:

1. It imposes a sequencing of the individual instructions sent. For example, in the situation illustrated hereinabove, it requires the transaction to be confirmed by the user before it

is signed.

2. It alone has the secret parameters for generating and authenticating these individual instructions. Thus it alone has the authentication and encryption keys for reading and decrypting the private key.

When the filter software executes in the secure microprocessor 3 of the terminal module 1 these properties enable a policy of access to the card 31 to be imposed which is not always completely imposed by the card itself, or the capacities of a card to be expanded (signature capacity delegated to the terminal module, use in a context not foreseen when initially deployed).

The advantages in terms of security of executing the filter software in the secure microprocessor of the terminal module or the integrated circuit card are possible only because the software executes in a secure environment, assuring that:

- the secrets contained in the filter software are not accessible because they are stored in the secure microprocessor 3, 29, 30 or 130,
- the confidentiality and the integrity of the filter software are preserved because the software is stored in the secure microprocessor 3, 29, 30 or 130.

If the terminal module 1 is a dedicated product having its own interfaces (display 4 and keyboard 5) the security objective is achieved because the software controlling exchanges of data with the user cannot be modified because it is permanently stored in the permanent memory 2c of the microcontroller 2 or securely stored in the microcontroller 29. Thus the user can confidently confirm the content of their transaction by means of the display 4 and the keyboard 5 and the need to verify the identity of the application or the source and the integrity of requests becomes optional.

Other mechanisms can further enhance the level of security of the chain of confidence between the secure microprocessor of the integrated circuit card, the secure microprocessor of the terminal module, when present, the standard microcontroller or the PC of the terminal module and the user. These mechanisms are:

A) secure downloading of the filter software;

B) authentication of the standard microcontroller by the secure microprocessor or (which amounts to the same thing but is more suitable in the case of a mode of execution of the terminal based on a PC) authentication of the interpreter software module I (20) by the filter software F (62) and/or setting up of a secure communication channel between these two microprocessors or the programs I and F;

C) protection of a secret by the standard microcontroller;

D) mutual authentication and setting up of a secure communication channel between the secure microprocessor of the integrated circuit card and the secure microprocessor of the terminal module;

E) authentication of the terminal module and where applicable of the terminal module/card combination; and

F) authentication of the microcircuit card by the terminal module.

A) Secure downloading of the filter software

The figure 10 flowchart illustrates the process of downloading an application program (filter software) into the secure microprocessor 3 or 29 of the module 1 or the secure microprocessor 30, 130 of a card 31, 131 in the reader 6. This downloading can be effected from a server Sap via the PC and the external connection interface 7 or the infrared link interface 8, for example, or directly by means of a telephone connection via the DTMF interface 9. The downloading can equally be effected into the secure microprocessor 3 or 29 (if the terminal module has one) from a microcircuit card inserted into the reader 6.

In step 32 the area of the memory 3d allocated to the application program to be received is empty and the microprocessor 3 is waiting to load the application program following a loading request.

The next step 33 corresponds to a procedure for authentication by the microprocessor 3 of the entity that will download the application program (sender). This authentication procedure can use encryption mechanisms well known to the skilled person, for example, such as symmetrical mechanisms using shared secret keys or asymmetrical mechanisms using private and public keys.

Step 34 is a test to determine if the authentication procedure has succeeded. If it has not, the message "access refused" is displayed on the screen 4 (step 42) and the program returns to step 32; if authentication has succeeded, the process for loading the application program begins in step 35.

Step 36 corresponds to storage in the EEPROM 3d of the data frames sent by the entity responsible for downloading.

Step 37 is a test to determine if downloading has finished: if not, the downloading program returns to step 36 and downloading continues; if it has finished, the microprocessor 3 verifies the integrity of the received data in step 38. To this end a message authentication code (MAC) can be associated with the downloaded program for verifying not only its integrity but also

its source. The MAC can be generated using a symmetrical cryptography mechanism (DES in chained CBC mode). The source and integrity can also be verified using an asymmetrical cryptography mechanism: a condensate of the downloaded software is signed by the sender using their private key; the secure microprocessor 3 then verifies the signature using the sender's public key.

Note that in this last example the public key in theory does not need to remain confidential. The security features of the microprocessor nevertheless assure the integrity of the software, preventing a hacker from modifying the software to eliminate the signature verification or simply to substitute for the public key initially provided a public key for which they know the associated private key.

If the test 39 indicates that the data received is correct, a flag indicating that the application program received is valid is generated in step 40. Otherwise the downloading program returns to the first step 32.

This process of loading the application software, and thus the filter software, into the secure reprogrammable memory (3d, 30a, 130a depending on the embodiment concerned) includes mechanisms for confirming the source and the integrity of the data received from the sender of the software. This prevents downloading by a hacker of filter software that could carry out transactions in the terminal module 1, 101 unknown to the user.

B) Authentication of the interpreter software module I, 20, 71 by the filter software F, 62 or, which amounts to the same thing in the corresponding mode of execution, authentication of the standard microcontroller 2 by the secure microprocessor and/or setting up of a secure communication channel between the programs or between the microprocessors

For a user to be totally confident in the terminal module they are using to carry out transactions it is necessary:

- to authenticate the data sent from the interpreter software 20, 71 to the secure microprocessor 3, 30 or 130 executing the filter software; and

- to assure that the data sent by the filter software to be displayed through the intermediary of the user's interpreter software of the terminal module 1, 101 can only be displayed by the latter.

When the means of controlling exchange of data with the user, i.e. the interpreter software 20, 71, is installed in the terminal module 1, 101 in a fixed manner and cannot be

modified, for example in the ROM 2c of the standard microcontroller 2, authenticating the software module is equivalent to authenticating the microcontroller.

Likewise, when the filter software is installed in secure processing means such as the secure microprocessor 3, the integrated circuit card or the secure server Ssec, in a manner such that it cannot be modified by an unauthorised person, authentication by these secure means is equivalent to authentication by the filter software itself.

In the following description the mechanisms for authentication of the software means controlling the interfaces or the interpreter software 20, 71 by the filter software will be described.

Various solutions verify these conditions.

A first solution consists in encrypting all the data exchanged between the interpreter software 20, 71 and the filter software.

A second solution is to have the interpreter software 20, 71 authenticated by the filter software and/or to set-up a secure communication channel between them.

These two solutions necessarily imply that at least one secret parameter known to the filter software F 62 is stored in the interpreter software 20, 71.

In the second solution the filter software F 62 authenticates the interpreter software 20, 71 using a conventional authentication process based on information sent by the interpreter software 20, 71 and combined with the secret parameter. At the level of the interpreter software 20, 71 this authentication procedure is executed by the software 72 (figure 8A) or the software 76 (figure 8B), depending on the embodiment of the terminal module concerned.

This authentication mechanism can equally be applied to messages exchanged between the programs to construct message authentication codes for guaranteeing the source and the integrity of each message transmitted.

In the case of the mode of execution described with reference to figure 4A, this solution nevertheless requires, for preference, physical protection of the link between the two microprocessors to be assured to prevent a hacker from reading the data exchanged and in particular the personal identification code (PIN) of the card, which the user may need to enter via the keyboard 5 to carry out transactions.

C) Protection of a secret parameter by the standard microcontroller 2

The foregoing description shows the necessity of storing at least one secret parameter in the interpreter software. The mode of execution of the terminal based on a PC, in which the interpreter software executes on the PC itself, therefore offers a limited degree of security for the

PC, although this degree of security is sufficient to prevent a virus substituting itself for the interpreter software. A higher degree of security is obtained by installing the interpreter software in the ROM 2c of the standard microcontroller 2. For enhanced security the secret parameter of the microcontroller 2 can be stored in the temporary memory when the product is manufactured or possibly on inserting the microprocessor 3 if it is removable, or on an integrated circuit card. The aim of this operation is to establish confidence between the two microprocessors. All necessary precautions must be taken at the time of this operation to assure the authenticity of the microcontroller 2 (operation effected by the manufacturer, operation protected by transport keys stored in the temporary memory of the microcontroller 2 by the manufacturer, and knowledge of which is a precondition for initialising said secret parameter). In addition, conventional mechanisms for detecting intrusion (contacts, etc) will be fitted to erase the temporary memory in the event of intrusion (by cutting off the power supply, etc).

D) Mutual authentication and setting up of a secure communication channel between the microprocessor of the integrated circuit card and the secure microprocessor of the terminal module

This mutual authentication and the setting up of the secure communication channel are effected by mechanisms identical to those used by the standard microcontroller 2 and the secure microprocessor executing the filter software, as described under B) above.

E) Authentication of the terminal module

It is important to guard against any attack on the combination of the keyboard 5, display 4 and secure microprocessor 3 with the aim of counterfeiting the terminal module, for example, substituting a counterfeit terminal module for a real terminal module in order to recover information entered by the user (keyboard spy), access the secrets of an integrated circuit card, falsify signatures.

To this end a mechanism can be added to enable the user to authenticate the terminal.

This objective is achieved by an automatic personalisation process.

Authentication of the terminal module alone

Personalisation can consist in calculating a password that is easy to remember and that is generated and displayed by the terminal in accordance with secret parameters contained in the microprocessor or microprocessors of the terminal when the user enters a PIN. If the terminal includes two microprocessors, for example, the password is stored in the secure microprocessor, encrypted using the PIN and a secret key X, and then sent to the microcontroller 2 where it is decrypted using the key X also stored in the microcontroller 2 and the PIN entered

by the user. This mechanism aims to protect against substitution of one of the two microprocessors.

The same principle can be applied to a card/terminal combination each time a microcircuit card is used with the terminal module. Personalisation can consist in the translation software calculating a password based on secret information held by the secure microprocessor of the card and secret information held by the terminal module, for example. The same principle as described hereinabove can be used to calculate the password. This password, generated the first time the terminal module is used in conjunction with the card and known to the user, is displayed on the screen 4 when the terminal module is used again with the card. The user can therefore verify and be assured that the terminal in their possession, consisting of the terminal module connected to the card, is authentic.

F) Authentication of the microcircuit card by the terminal module

To enhance further the security of the transaction system in accordance with the invention, a conventional authentication process can be used for authentication by the terminal module 1, 101 of the microcircuit card used. An authentication process of the above kind prevents the user's personal identification number (PIN), entered by the latter into the module 1, 101 via the keyboard 5 to execute a secured transaction, from being captured by a counterfeit card substituted by a hacker for the user's authentic card and subsequently recovered by the hacker to read the PIN off the counterfeit card. This authentication can be effected by a means of a conventional challenge/response type mechanism, for example, using a secret shared between the card and the terminal module and symmetrical cryptography or, as already described, using a private key stored by the card enabling the challenge to be encrypted using an asymmetrical algorithm, the terminal module verifying the response using its public key.

The architecture of the transaction system and the security mechanisms described hereinabove make transactions effected by means of the terminal module 1, 101 highly secure.

The terminal module:

- expands the nature of the truly secure services that a microcircuit card can provide, thanks to the keyboard 5, the screen 4 and the protection of data exchanged with the user; and
- enables the card to be used in a non-secure environment (PC susceptible to viruses or pirate programs), by hermetically isolating it from this environment by means of a software and/or hardware architecture strictly controlling access to the card, i.e. controlling commands sent to the cryptographic functions on the card.

The terminal module can take various forms, for example:

- an integrated circuit card reader for connection to a computer via various interfaces (PCMCIA, etc) or not (connection to a server via modem only);
- a computer (PC) the user interfaces of which consist in the screen and the keyboard of the PC and which includes an integrated circuit card reader. The PC will include software and/or hardware means (such as a secure second microprocessor, the standard microprocessor consisting of the PC itself) for assuring the integrity and the confidentiality of the filter software. By computer is meant a PC or a PDA (Personal Digital Assistant);
- a keyboard, possible provided with an LCD display screen, incorporating a secure microprocessor and an integrated circuit card interface;
- a telephone, possible equipped with a display, incorporating a secure microprocessor and an integrated circuit card interface;
- a cable TV network decoder (set-top box) incorporating an integrated circuit card reader connected to a TV, the telephone, a keyboard or possibly the remote controller for the decoder or the TV providing the user interface;
- more generally, any equipment that can be rendered secure by incorporating a secure microprocessor in which a sensitive application can be installed or by incorporating an integrated circuit card interface enabling said equipment to be controlled by an application installed on an integrated circuit card.

The whole of the foregoing description describes a terminal to be used with an integrated circuit card or smart card. The card referred to is in fact a tool enabling the use of cryptographic functions personalised to one user by means of at least one secret parameter. The object of the invention is clearly not limited to a given form of tool such as an integrated circuit card. The invention also covers the use of personal security devices offering functions equivalent to those of an integrated circuit card but presented in a different form, such as the "iButton", "Java Ring" and "token" products.

CLAIMS

1. A terminal for execution of secure electronic transactions by a user in conjunction with at least one application installed on an electronic unit, said terminal comprising:

- a terminal module including at least:

* first interface means with said application for receiving from it requests relating to said transactions,

* second interface means with said user;

* third interface means with a personal security device,

* first data processing means comprising at least first software means for controlling said interface means, and

- a personal security device including at least second secure data processing means comprising at least second software means for executing elementary commands and means for executing cryptographic computations,

characterised in that:

- said terminal (1, 31; 101, 131) is adapted to receive said requests from said application (Fap) installed on said electronic unit (Sap; PC) in the form of high-level requests independent of said personal security device,

- at least one of said terminal module (1; 101) and said personal security device comprises :

* at least one reprogrammable memory (3d; 30a; 102b; 130a; Ssec)for storing at least one filter program (F, 62) translating said high-level requests into at least one of either :

(i) at least an elementary command or a sequence of elementary commands that can be executed by said second software means (80-84) of said second data processing means (30; 130), or

(ii) at least one sequence of data exchanges between said terminal module (1 ; 101) and said user via said second interface means (4, 5), which can be executed by said first software means (I, 20, 71) of said first data processing means (2; 29; 102), and

* means for protecting said filter program (F, 62) to prevent an unauthorised entity from either reading and/or modifying said filter program, and

- at least one of said first and said second data processing means (3; 29, 30; 102; 130; Ssec) comprise a data processing device for executing said filter program (F, 62).

2. A terminal according to claim 1 characterised in that said device for executing the

filter program comprises first means for identifying and/or authenticating said application (Fap) installed on said electronic unit (Sap; PC) or the source of said requests sent by said application.

3. A terminal according to claim 2 characterised in that said data processing device for executing said filter program (F, 62) comprises means for verifying the integrity of data received from said application (Fap).

4. A terminal according to any one of claims 1 to 3 characterised in that said data processing device for executing said filter program (F, 62) comprises centralised means (Ssec) for controlling conditions of use of services of the personal security device (31) in accordance with said application (Fap) and/or the user.

5. A terminal according to any one of claims 1 to 4 characterised in that said data processing device for executing said filter program (F, 62) comprises:

- means for commanding loading in a secured manner of said filter program into said programmable memory via said first or said third interface means from an entity external to said module, and

- first access control means for authorising said loading of said filter program only in response to at least one predefined condition.

6. A terminal according to any one of claim 1 to 5 characterised in that it comprises second means for authenticating said first data processing means (2; 3; 29; Ssec) by said second data processing means (30; 130).

7. A terminal according to any one of claims 1 to 6 characterised in that it comprises third means for authenticating said second data processing means (30; 130) by said first data processing means (3; 29).

8. A terminal according to claim 6 or claim 7 characterised in that it comprises a first communication channel (6) between said first data processing means (2; 3; 29) and said second data processing means (30; 130) and first means for securing said first communication channel.

9. A terminal according to any one of claims 1 to 8 characterised in that it comprises fourth means for authentication of said terminal module (1; 101) by said user, independently of said personal security device (31; 131).

10. A terminal according to claim 9 characterised in that said fourth authentication means comprise means for calculating by said first data processing means (2; 3; 29) and for presentating to said user via said second interface means (4) a password known to said user and calculated on the basis of a first secret parameter stored in said first data processing means (2; 3; 29).

11. A terminal according to any one of claims 1 to 10 characterised in that it comprises fifth means for conjoint authentication of said terminal module (1; 101) and said personal security device (31; 131) by said user.

12. A terminal according to claim 11 characterised in that said fifth authentication means comprise means for calculating by said device for executing said filter program (3; 29; 31; 131) and for presentating to said user via said second interface means (4) a password known to said user and calculated on the basis of at least second and third secret parameters stored respectively in memory in said first data processing means (2; 3; 29) and in memory in said second data processing means (30; 130).

13. A terminal according to any one of claims 1 to 12 characterised in that said terminal module (1) includes said programmable memory (3d) for loading and storing said filter program (F, 62).

14. A terminal according to claim 13 characterised in that said filter program (F, 62) generates first commands for implementing said at least one sequence of exchanges of data between said terminal module (1) and said user and said first data processing means comprise a first microprocessor (2; 102) for controlling said interface means (4-9) programmed by virtue of said first software means (20, 71) for controlling said interface means to execute said first commands generated by said filter program (F, 62), and a second secure microprocessor (3) of the integrated circuit card type disposed in said terminal module and including said programmable memory (3d), said second microprocessor (3) executing said filter program (F, 62) to control said at least one sequence of exchanges of data by means of said first commands sent to said first microprocessor (2) and for applying said at least one elementary command or sequence of elementary commands to said second data processing means.

15. A terminal according to claim 14 characterised in that said first software means (20, 71) for controlling the interface means include at least a fourth secret parameter, said second microprocessor (3) being controlled by said filter program (F, 62) to authenticate said first software means (20, 71) for controlling the interface means on the basis of information sent by said first microprocessor (2) and combined at least with said fourth secret parameter.

16. A terminal according to claim 15 characterised in that it comprises a second communication channel (12) between said first software means (20, 71) for controlling the interface means and said second microprocessor (3) and second means for securing said second communication channel.

17. A terminal according to claim 16 characterised in that said second securing means

comprise means for encryption and decryption by said first software means (20, 71) and by said second microprocessor (3), of data sent on said second communication channel (12) on the basis of at least a fifth secret parameter stored in memory in said first and second data processing means.

18. A terminal according to claim 16 or claim 17 characterised in that said second securing means comprise first physical means for protecting said second communication channel (12) against intrusion.

19. A terminal according to any one of claims 15 to 18 characterised in that said first microprocessor (2) includes a temporary memory (2b) for storing said secret parameter and second means for physically protecting said temporary memory (2b) against intrusion.

20. A terminal according to any one of claims 14 to 19 characterised in that said second microprocessor (2) is a microcontroller.

21. A terminal according to claim 13 characterised in that said filter program generates first commands for implementing said at least one sequence of data exchanges between said terminal module and said user and said first data processing means comprise said device for executing said filter program and consist in a secure microprocessor (29) adapted to:

* execute said filter program (F, 62) for translating and converting said high-level requests into at least one sequence of data exchanges between the terminal module and the user and/or into at least one elementary command or a sequence of elementary commands that can be executed by said second software means of said second data processing means (31),

* control said interface means (4-9) using said first commands generated by said filter program to implement said at least one sequence of exchanges between said terminal module (1) and said user.

22. A terminal according to claim 21 characterised in that said microprocessor (29) includes said programmable memory.

23. A terminal according to claim 21 characterised in that said programmable memory is external to said microprocessor (29).

24. A terminal according to claim 23 characterised in that said filter program (F, 62) is stored in encrypted form in said programmable memory and in that said microprocessor (29) comprises means for reading, decrypting and executing said filter program.

25. A terminal according to any one of claims 14 to 24 characterised in that said second data processing means of said personal security device (31) comprise a second data processing device (30) for secure execution of a filter program and a programmable memory

(30a) for loading and storing said filter program (62), said first software means of said first data processing means being adapted to receive said commands for implementing said at least one sequence of exchange of data from either of said filter program executing devices (3; 29; 31) installed in said module and said personal security device, respectively.

26. A terminal according to any one of claims 13 to 25 characterised in that:

- said filter program (F, 62) comprises at least one secret parameter,

- said second data processing means (30) comprise second means of conditional access control for authorising execution of said cryptographic computations in response to elementary commands generated by said filter program (F, 62) only if at least a second predefined condition depending on said secret parameter is satisfied.

27. A terminal according to any one of claims 1 to 12 characterised in that said personal security device (131) includes said programmable memory (130a) for loading and storing said filter program (F, 62).

28. A terminal according to claim 27 characterised in that said filter program (F, 62) generates first commands for implementing said at least one sequence of exchanges of data between said terminal module (1) and said user and said first data processing means comprise a first microprocessor (2; 102) for controlling said interface means (4-9), programmed by said first software means (20, 71), to execute said first commands generated by said filter program (F, 62), and said second data processing means comprise a secure second microprocessor (130) of the integrated circuit card type disposed in said personal security device (131) and including said programmable memory (130a), said second microprocessor (130) executing (i) said filter program (F, 62) for controlling said at least one sequence of exchanges of data by means of said first commands sent to said first microprocessor (2; 102), and (ii) said elementary commands.

29. A terminal according to claim 6 and claim 28 characterised in that said first software means (20, 71) for controlling said interface means include at least one secret parameter and said second microprocessor (130) of said personal security device (131) is controlled by said filter software (62) to authenticate said first microprocessor (2) on the basis of information sent by said first microprocessor (2) and combined at least with said secret parameter.

30. A terminal according to claim 28 or claim 29 characterised in that said second microprocessor (130) of said personal security device (131) is adapted to command the loading of said filter program (F, 62) into said programmable memory (130a) via said first interface

means (7-9) and said third interface means (6) with said personal security device (131).

31. A terminal according to any one of claims 13 to 30 characterised in that said terminal module (1; 101) is an integrated circuit card reader and said personal security device is an integrated circuit card (31; 131).

32. A terminal according to claim 13 characterised in that said terminal module (1) comprises a personal computer (102) and in that said reprogrammable memory is included in the hard disk (102b) of said computer.

33. A terminal according to claim 32 and any one of claims 14 to 17 characterised in that said first microprocessor is the microprocessor (102c) of said personal computer (102), said personal computer (102) being also interfaced to said secure microprocessor (3).

34. A terminal according to claim 32 characterised in that said filter program (F) comprises a loading/decryption first module (Fcd) and an encrypted second module (Fchi) for said translation of high-level requests, said first module (Fcd) commanding the loading of said second module (Fchi) into RAM of said computer (102) and its decryption for execution of said filter program by said computer.

35. A terminal according to claim 32 characterised in that said filter program (F) comprises at least one first module (F-PC) installed on said personal computer (102) and at least one second module (F-SE) installed on a security server (Ssec), said personal computer (102) and said security server (Ssec) being connected by a secure communication channel (CS) enabling protected exchange of data between said modules.

36. A terminal according to any one of claims 32 to 35 characterised in that said personal security device (31) is an integrated circuit card.

37. A system for performing secure transactions characterised in that it comprises at least one terminal (1, 31; 101, 131) according to any one of claims 1 to 36 and at least one electronic unit (Sap; PC) including means for transmitting said high-level requests to said terminal(1, 31; 101, 131).

38. A system according to claim 37 characterised in that it comprises a plurality of terminals (1, 31; 101, 131), at least one server (S) constituting said electronic unit and means (CR) for sending digital data between said server (S) and said terminals.

TITLE: Terminal and system for performing secure electronic transactions.

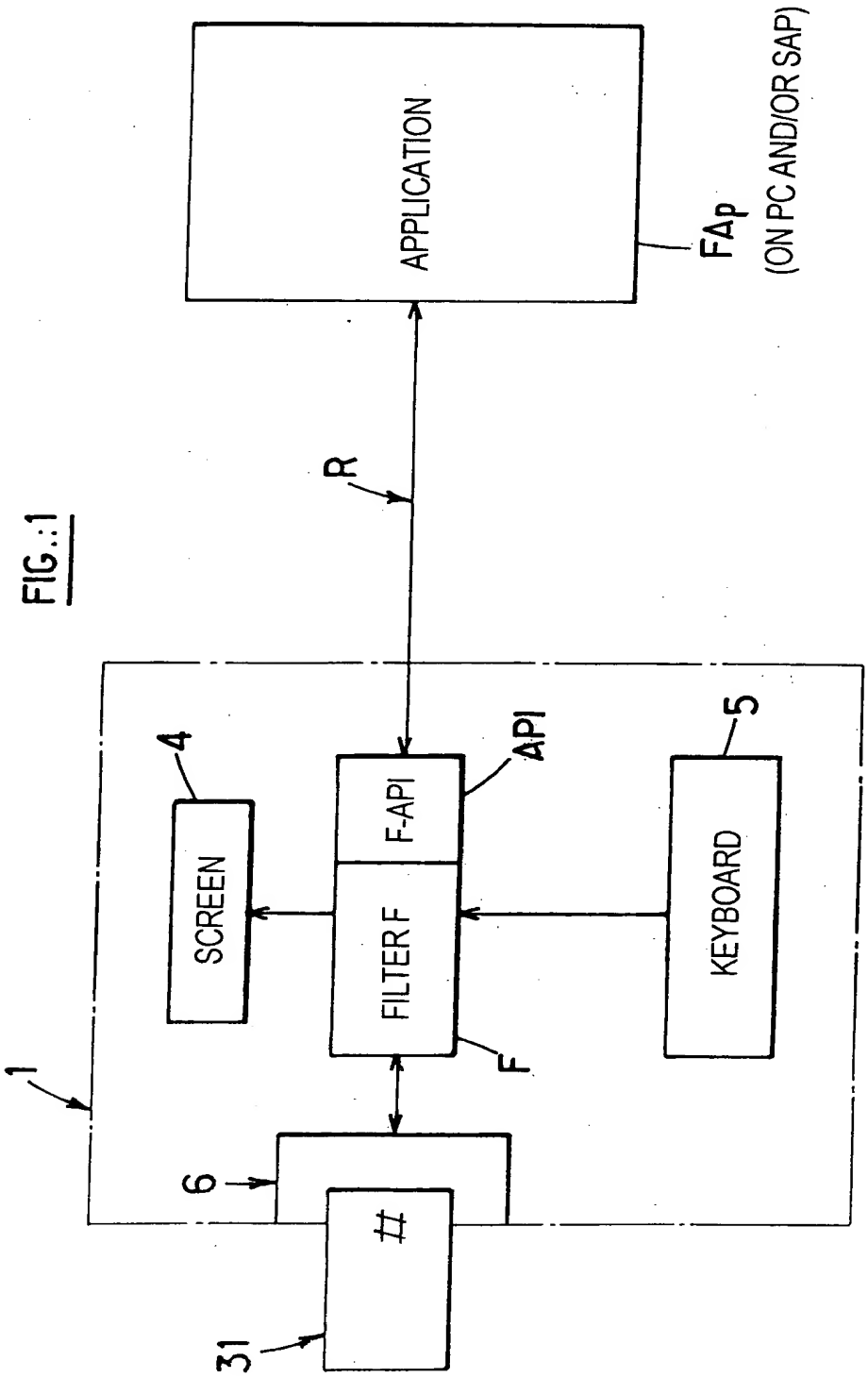
ABSTRACT OF THE DISCLOSURE

The terminal includes a terminal module (1) and a person security device (31). The terminal module (1) is adapted to receive requests from an application (Fap) installed on an electronic unit in the form of high-level requests independent of the module (1) and of said personal security device (31).

The terminal module (1) and/or the personal security device (31) includes a reprogrammable memory for storing and means for executing a filter program (F) translating the high-level requests into at least one of either (i) at least one sequence of exchanges of data between the terminal module (1) and the user or (ii) at least one elementary command or a sequence of elementary commands that can be executed by the personal security device, together with means for protecting said filter program (F, 62) to prevent any modification of said program by an unauthorised person. The filter program comprises means for identifying and/or authenticating the source of requests sent by said application (Fap) installed in said unit.

FIGURE 1

FIG.:1


APPLICATION
FAp
(ON PC AND/OR SAP)
R
1
4
SCREEN
F-API
API
FILTER F
F
5
KEYBOARD
6
#
31

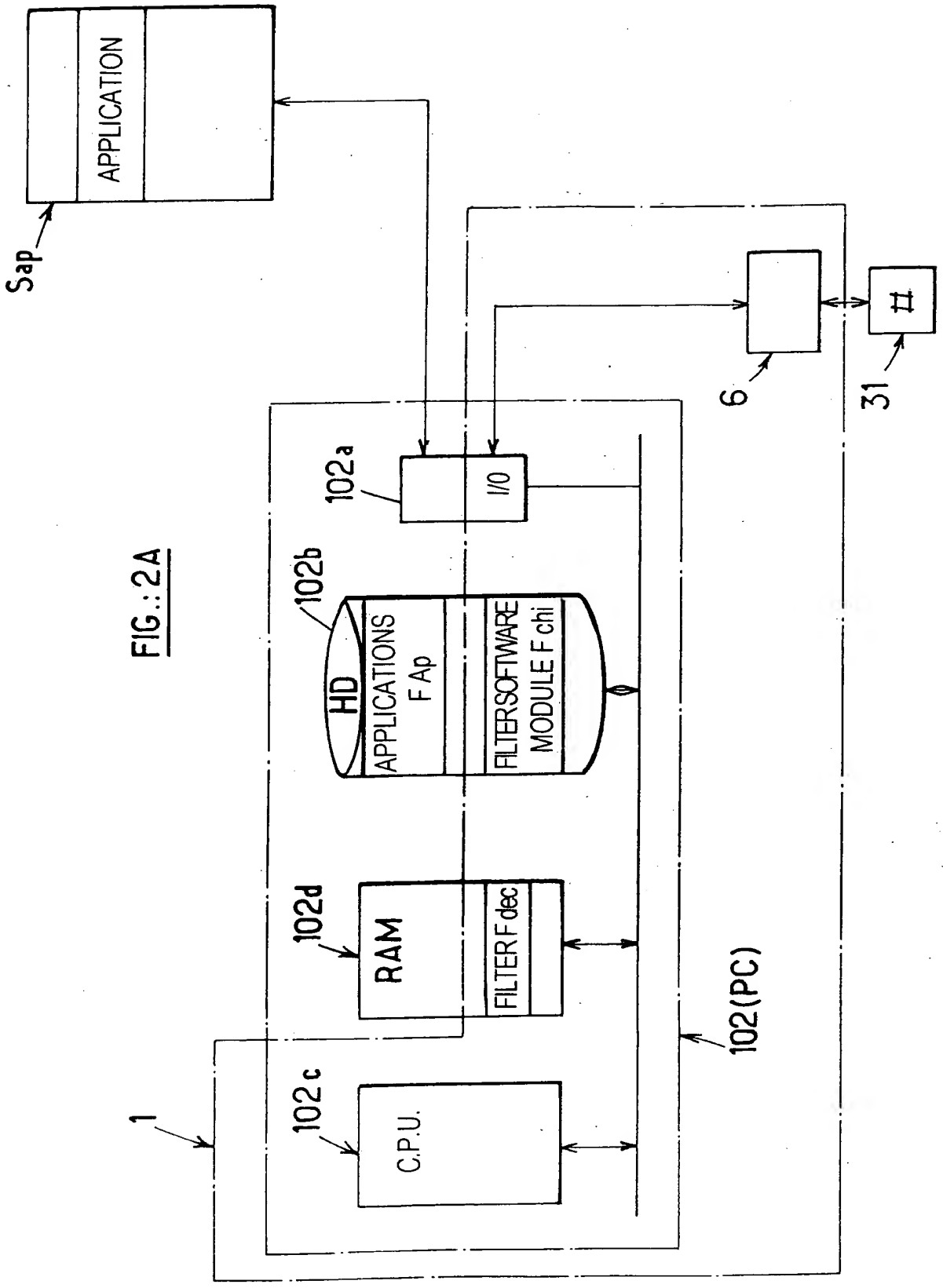
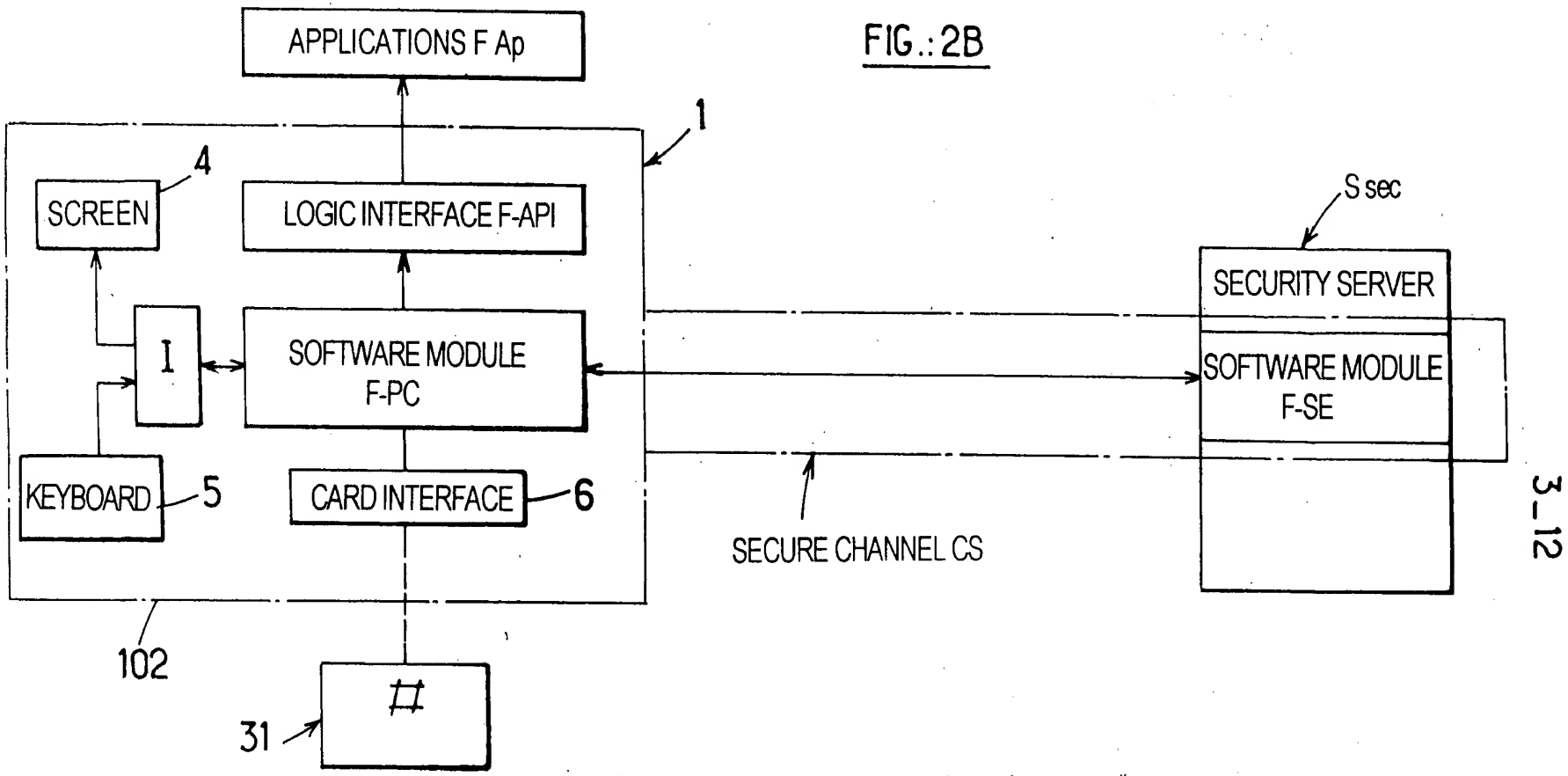

APPLICATION
Sap
6
31
102a
I/O
102b
HD
APPLICATIONS
F Ap
FILTERSOFTWARE
MODULE F chi
102d
RAM
FILTER F dec
102c
C.P.U.
1
102(PC)

FIG.: 2A

FIG.: 2B


APPLICATIONS F Ap
1
4
SCREEN
LOGIC INTERFACE F-API
S sec
SECURITY SERVER
I
SOFTWARE MODULE
F-PC
SOFTWARE MODULE
F-SE
KEYBOARD
5
CARD INTERFACE
6
SECURE CHANNEL CS
3_12
102
31

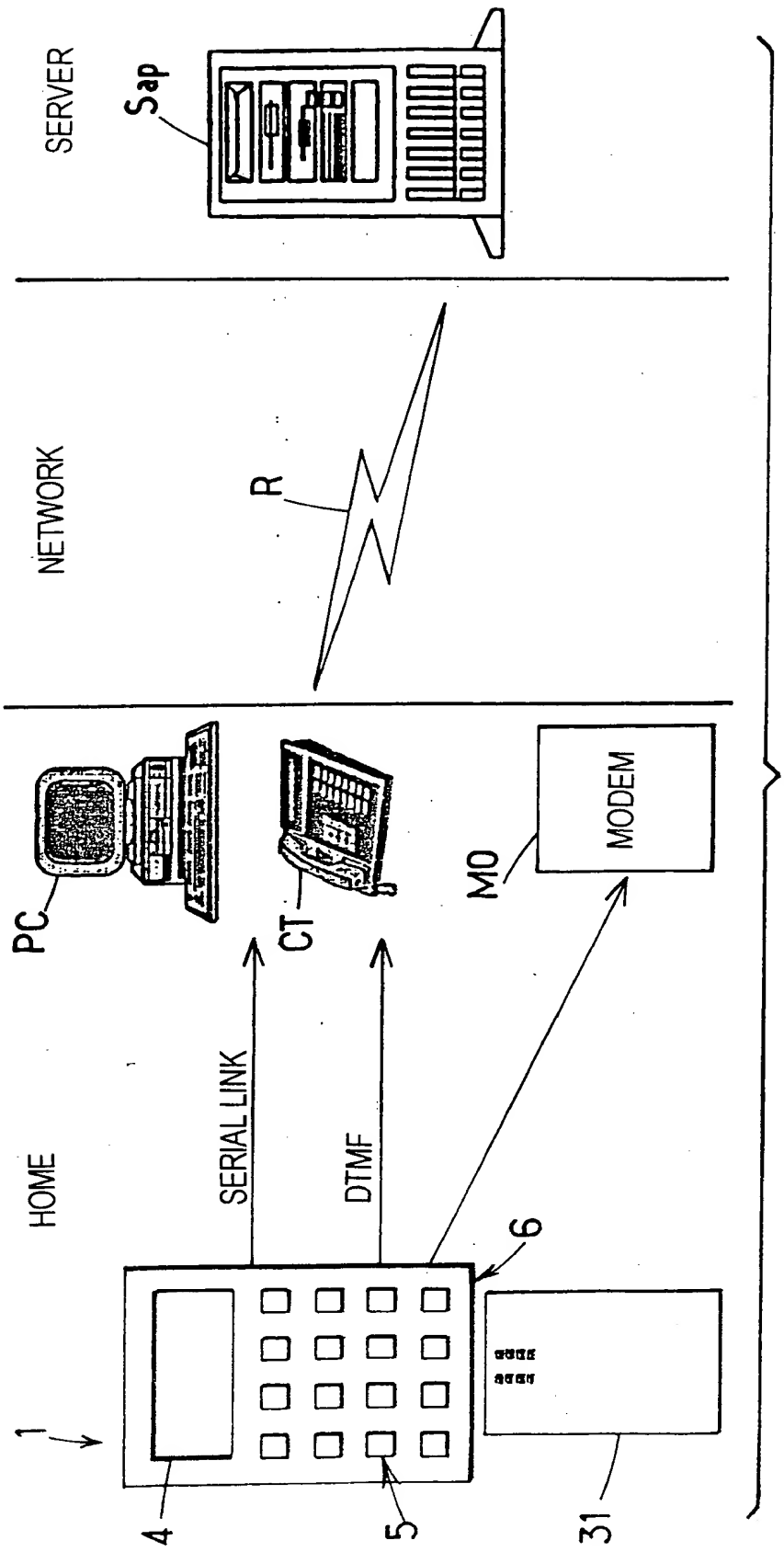

SERVER
Sap
NETWORK
R
HOME
SERIAL LINK
DTMF
PC
CT
MO
MODEM
1
4
5
6
31

FIG.:3

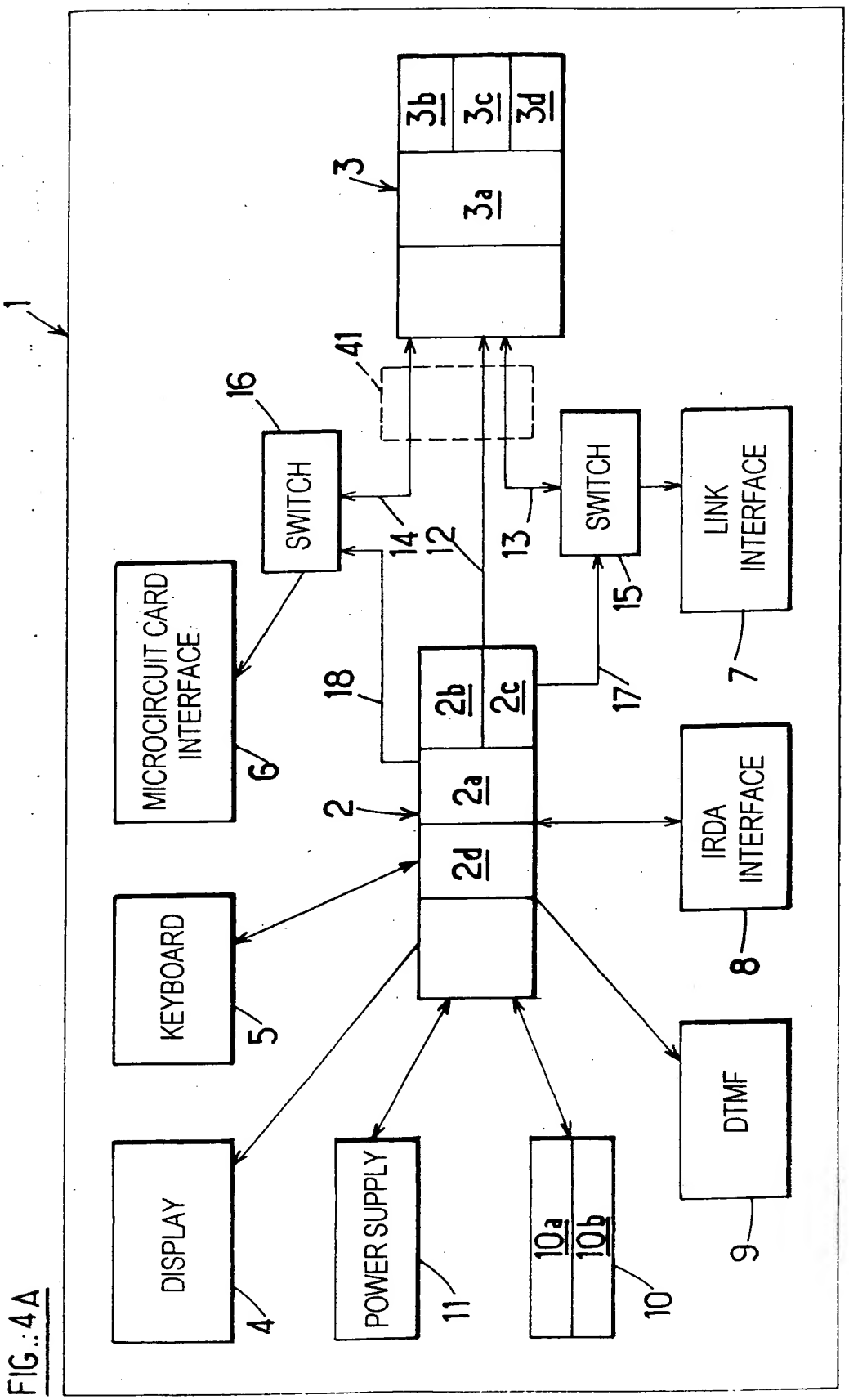

1
3
3a
3b
3c
3d
41
16
SWITCH
14
12
13
SWITCH
15
LINK INTERFACE
7
MICROCIRCUIT CARD INTERFACE
6
18
2
2a
2b
2c
2d
17
IRDA INTERFACE
8
KEYBOARD
5
DISPLAY
4
POWER SUPPLY
11
10a
10b
10
DTMF
9

FIG.:4A

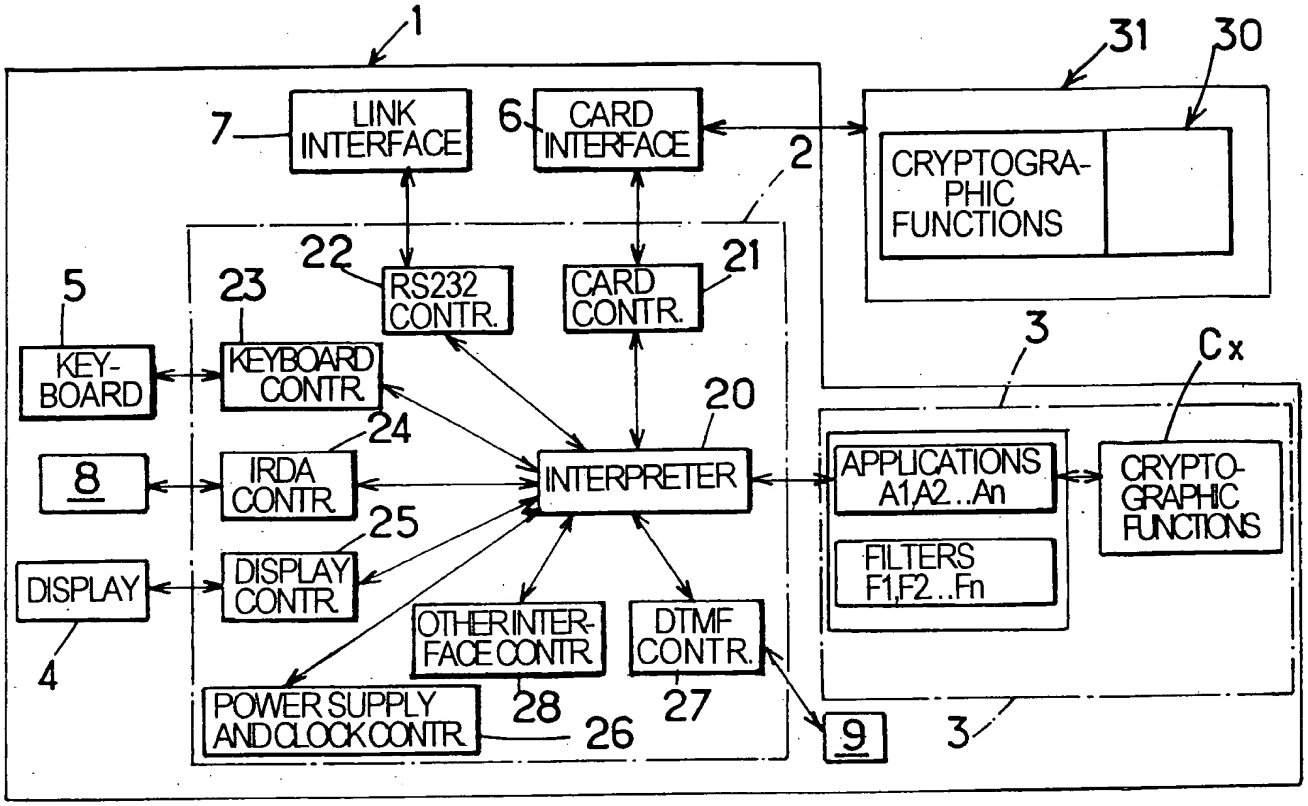
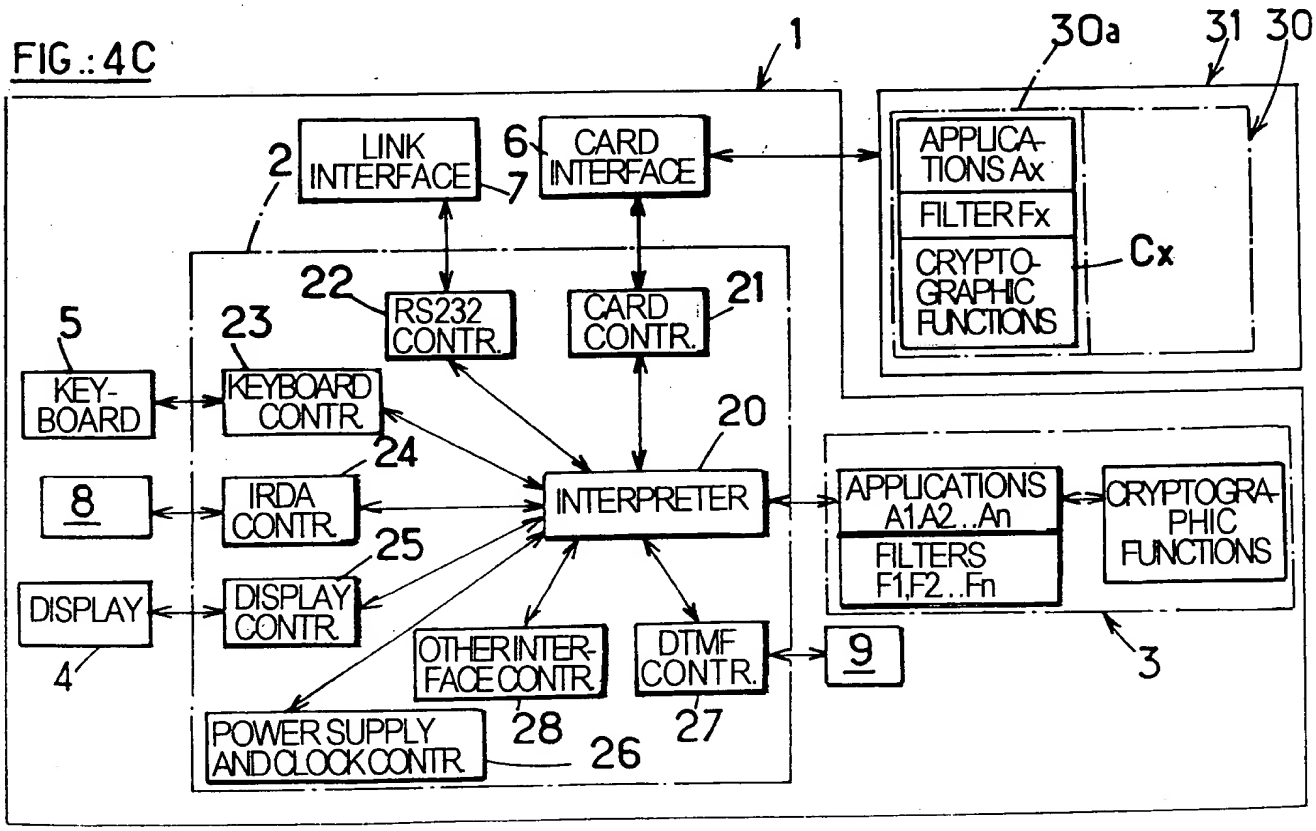

1
31
30
7
LINK INTERFACE
6
CARD INTERFACE
2
CRYPTOGRA-PHIC FUNCTIONS
22
RS232 CONTR.
CARD CONTR.
21
5
23
KEY-BOARD
KEYBOARD CONTR.
3
Cx
20
24
8
IRDA CONTR.
INTERPRETER
APPLICATIONS A1,A2..An
CRYPTO-GRAPHIC FUNCTIONS
25
FILTERS F1,F2..Fn
DISPLAY
DISPLAY CONTR.
OTHER INTER-FACE CONTR.
DTMF CONTR.
4
POWER SUPPLY AND CLOCK CONTR.
28
27
26
9
3

FIG.: 4B

FIG.: 4C


1
30a
31
30
2
LINK INTERFACE
6
7
CARD INTERFACE
APPLICA-TIONS Ax
FILTER Fx
CRYPTO-GRAPHIC FUNCTIONS
Cx
22
RS232 CONTR.
CARD CONTR.
21
5
23
KEY-BOARD
KEYBOARD CONTR.
20
24
8
IRDA CONTR.
INTERPRETER
APPLICATIONS A1,A2..An
CRYPTOGRA-PHIC FUNCTIONS
25
FILTERS F1,F2..Fn
DISPLAY
DISPLAY CONTR.
OTHER INTER-FACE CONTR.
DTMF CONTR.
9
4
POWER SUPPLY AND CLOCK CONTR.
28
27
26
3

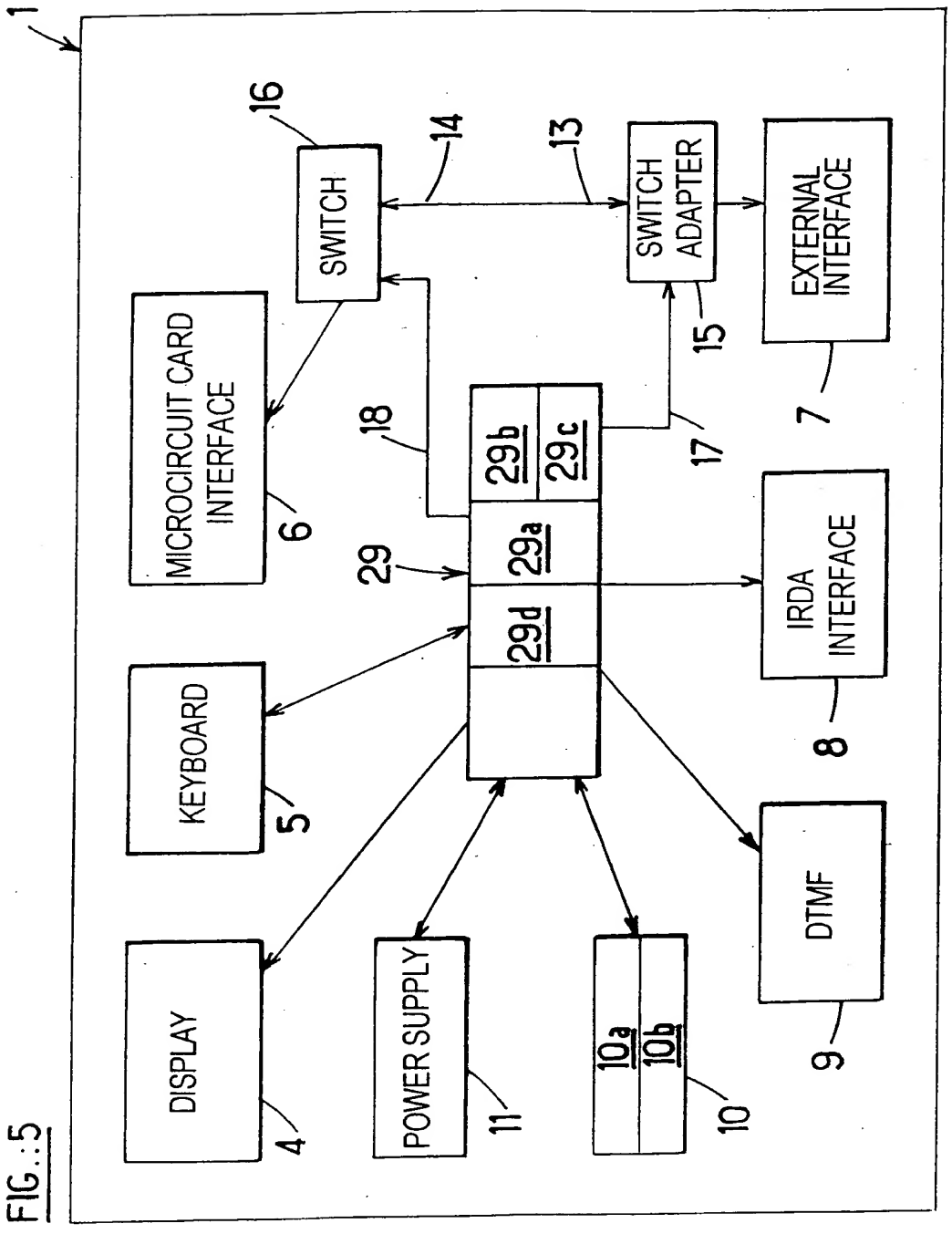

1
16
SWITCH
14
13
SWITCH ADAPTER
EXTERNAL INTERFACE
MICROCIRCUIT CARD INTERFACE
6
18
29b
29c
17
15
7
29
29a
29d
IRDA INTERFACE
8
KEYBOARD
5
DISPLAY
4
POWER SUPPLY
11
10a
10b
10
DTMF
9

FIG.:5

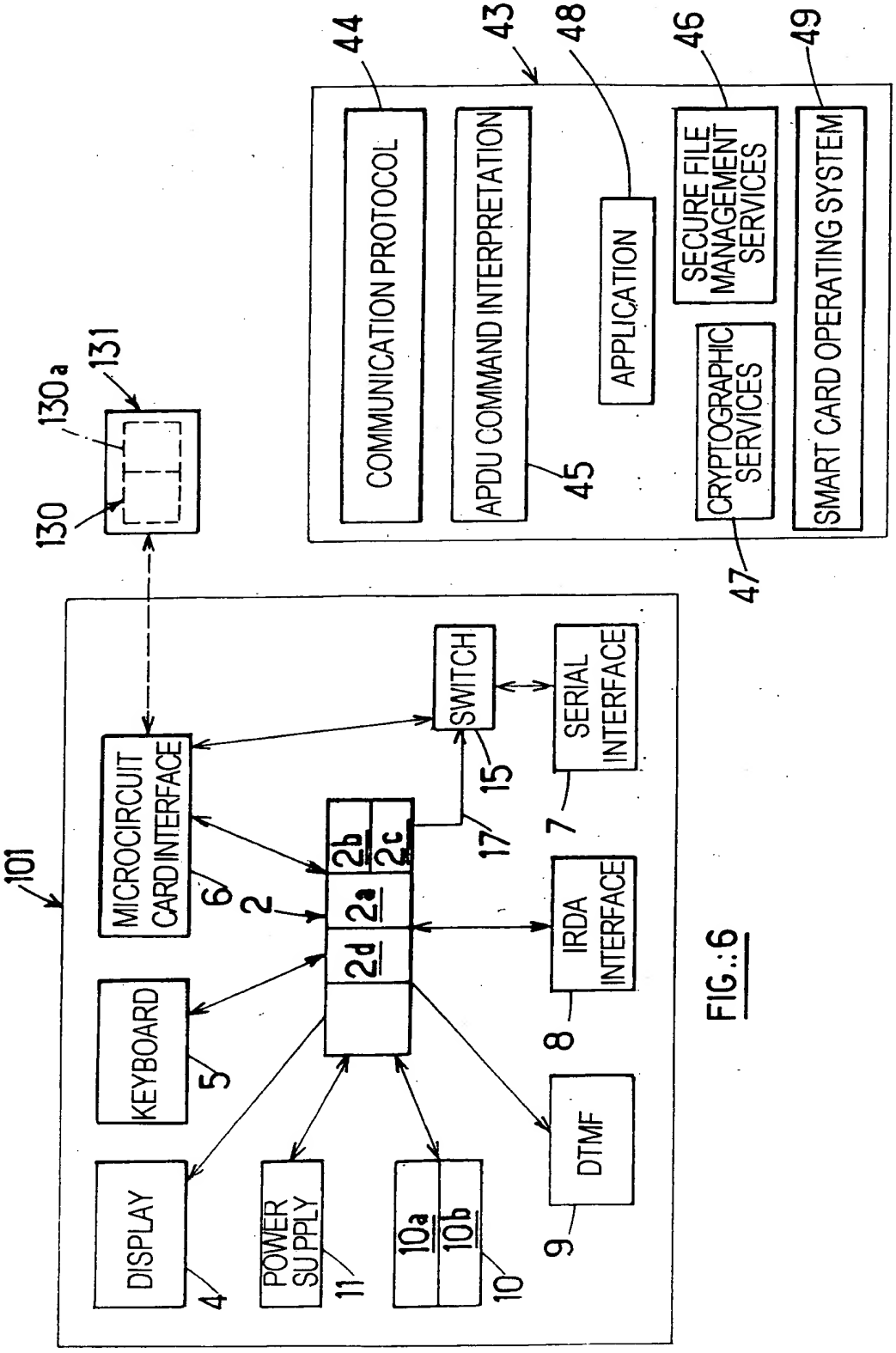

101
MICROCIRCUIT CARD INTERFACE
6
2
2b
2c
2a
2d
SWITCH
15
17
SERIAL INTERFACE
7
IRDA INTERFACE
8
DTMF
9
KEYBOARD
5
DISPLAY
4
POWER SUPPLY
11
10a
10b
10
130
130a
131
44
43
48
46
49
COMMUNICATION PROTOCOL
APDU COMMAND INTERPRETATION
45
APPLICATION
SECURE FILE MANAGEMENT SERVICES
CRYPTOGRAPHIC SERVICES
47
SMART CARD OPERATING SYSTEM

FIG.:6

FIG.:7

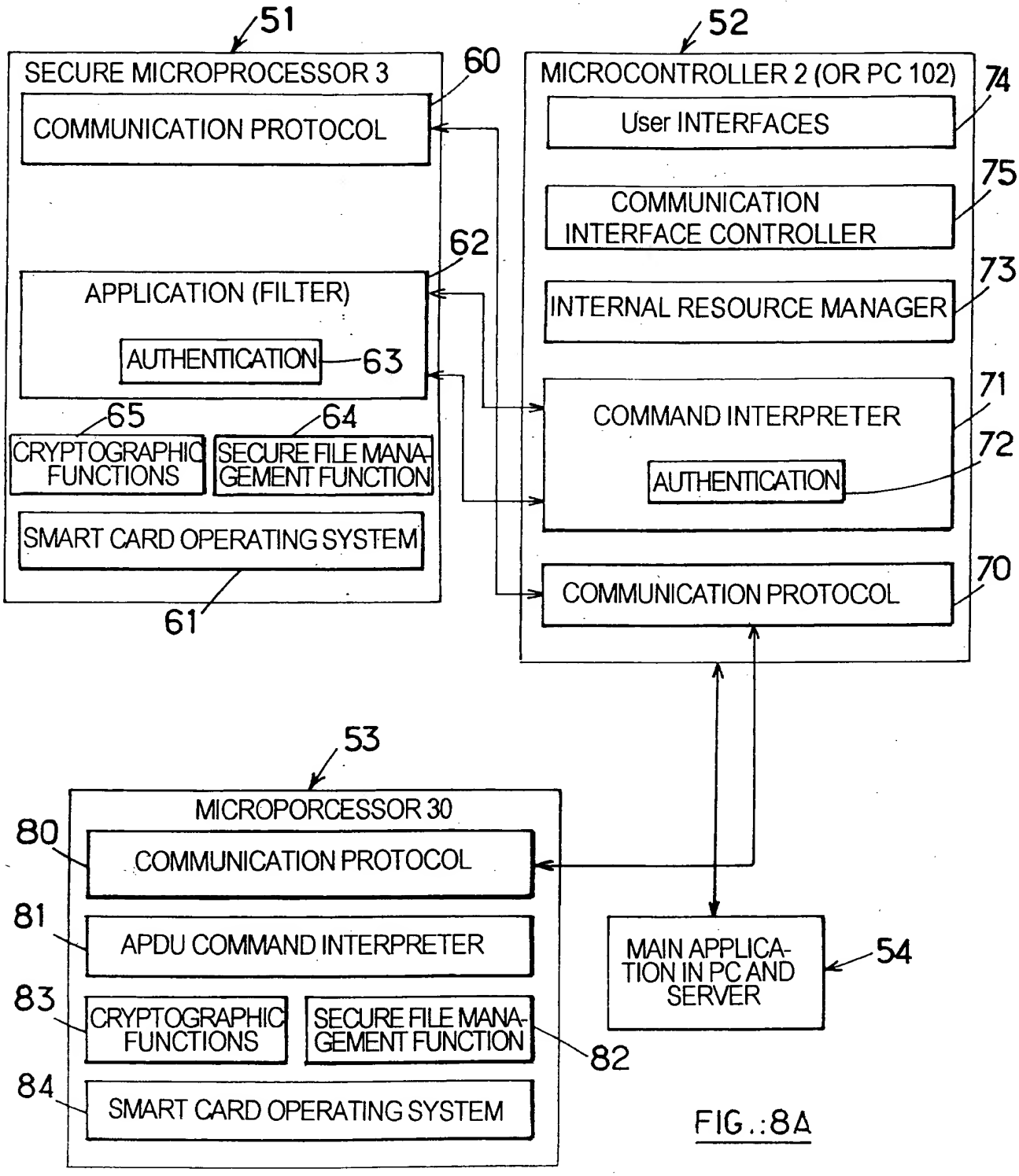

51
SECURE MICROPROCESSOR 3
60
COMMUNICATION PROTOCOL
62
APPLICATION (FILTER)
AUTHENTICATION
63
65
64
CRYPTOGRAPHIC FUNCTIONS
SECURE FILE MANAGEMENT FUNCTION
SMART CARD OPERATING SYSTEM
61
52
MICROCONTROLLER 2 (OR PC 102)
74
User INTERFACES
75
COMMUNICATION INTERFACE CONTROLLER
73
INTERNAL RESOURCE MANAGER
71
COMMAND INTERPRETER
72
AUTHENTICATION
70
COMMUNICATION PROTOCOL
53
MICROPORCESSOR 30
80
COMMUNICATION PROTOCOL
81
APDU COMMAND INTERPRETER
83
CRYPTOGRAPHIC FUNCTIONS
SECURE FILE MANAGEMENT FUNCTION
82
84
SMART CARD OPERATING SYSTEM
MAIN APPLICATION IN PC AND SERVER
54

FIG.:8A

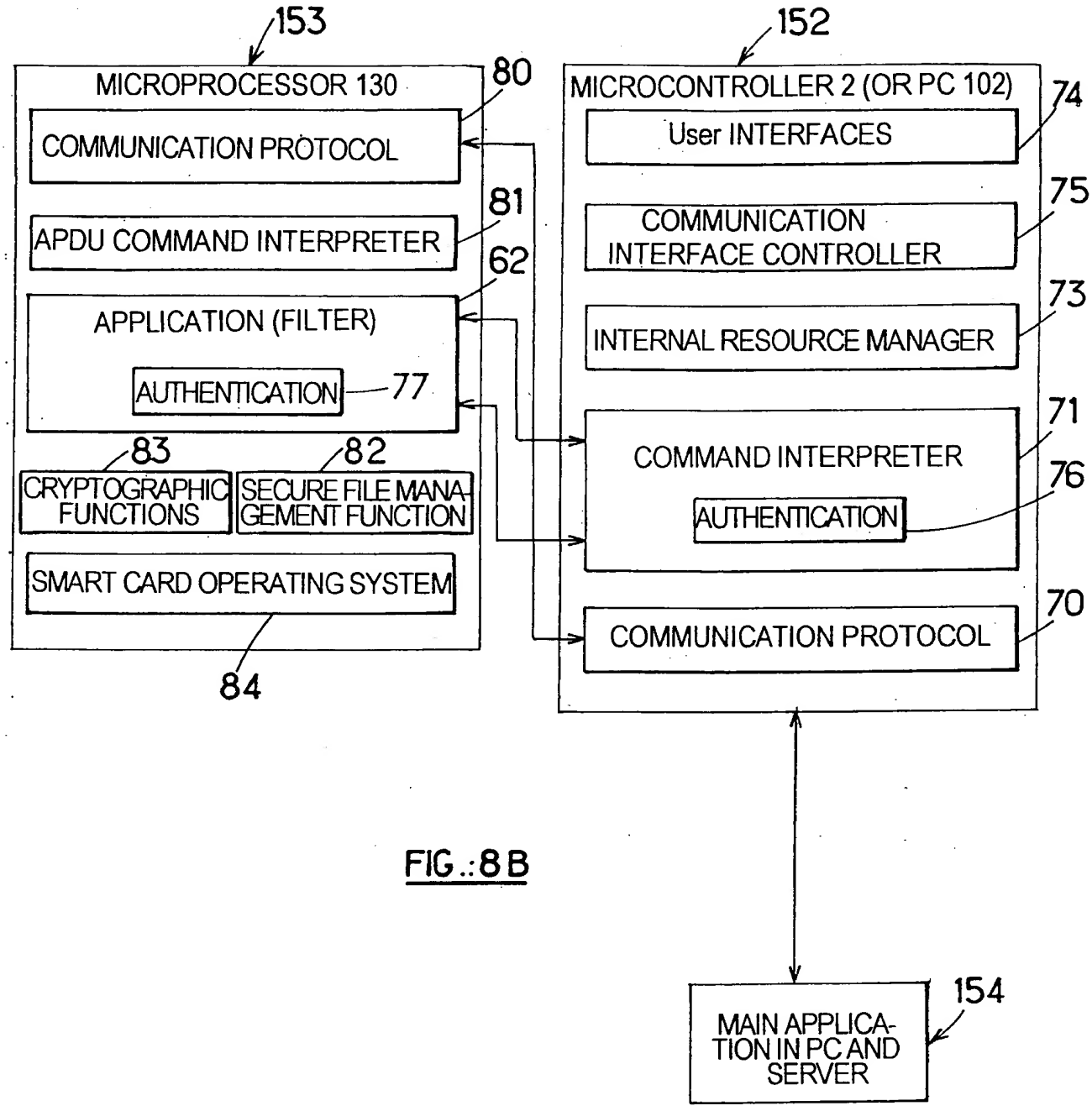

153
MICROPROCESSOR 130
80
COMMUNICATION PROTOCOL
81
APDU COMMAND INTERPRETER
62
APPLICATION (FILTER)
AUTHENTICATION
77
83
82
CRYPTOGRAPHIC FUNCTIONS
SECURE FILE MANAGEMENT FUNCTION
SMART CARD OPERATING SYSTEM
84
152
MICROCONTROLLER 2 (OR PC 102)
74
User INTERFACES
75
COMMUNICATION INTERFACE CONTROLLER
73
INTERNAL RESOURCE MANAGER
71
COMMAND INTERPRETER
76
AUTHENTICATION
70
COMMUNICATION PROTOCOL
154
MAIN APPLICATION IN PC AND SERVER

FIG.:8B

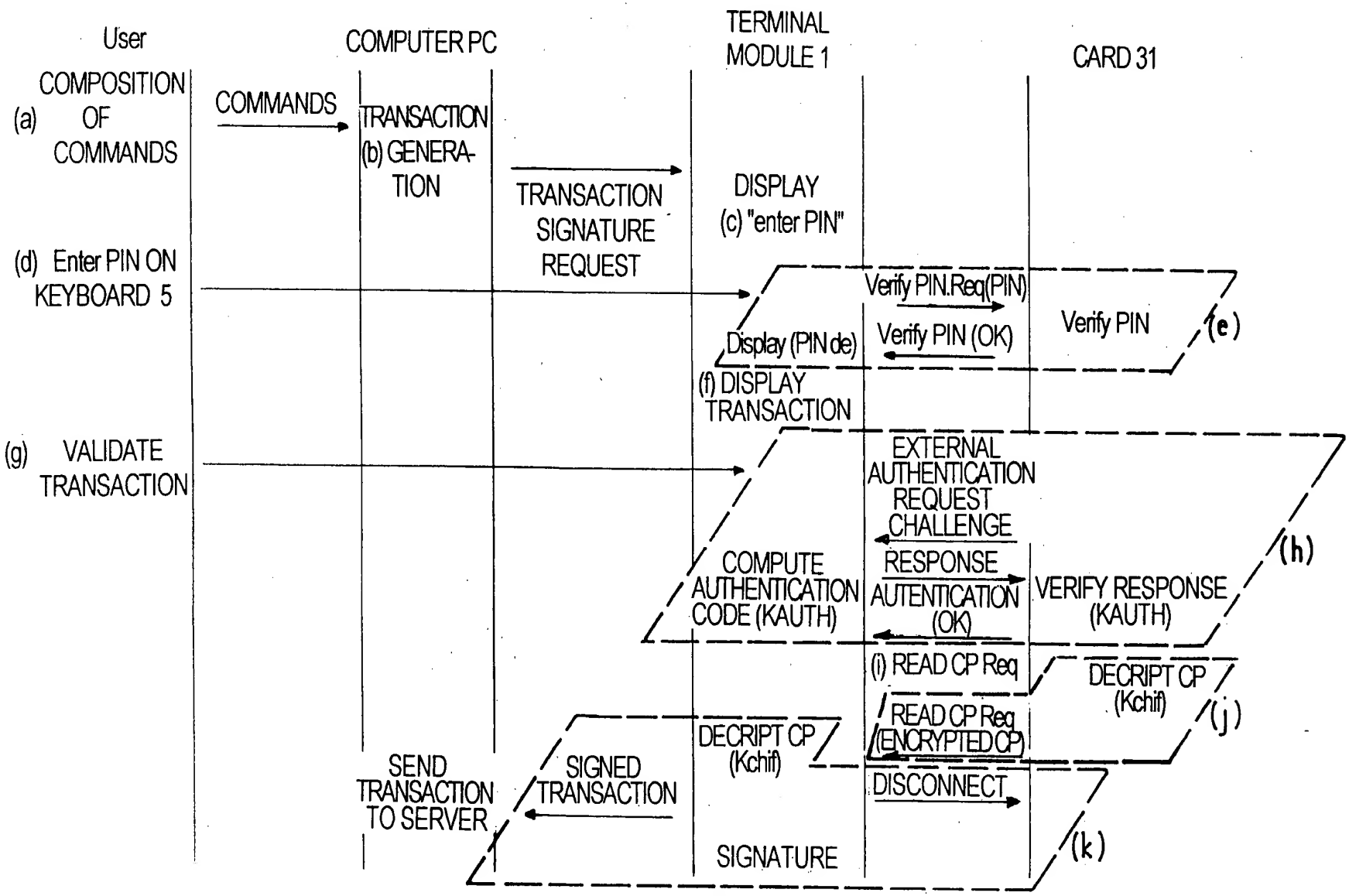

User
COMPUTER PC
TERMINAL MODULE 1
CARD 31
COMPOSITION OF COMMANDS
(a)
COMMANDS
TRANSACTION (b) GENERATION
TRANSACTION SIGNATURE REQUEST
DISPLAY (c) "enter PIN"
(d) Enter PIN ON KEYBOARD 5
Verify PIN.Req(PIN)
Verify PIN
Verify PIN (OK)
Display (PIN de)
(e)
(f) DISPLAY TRANSACTION
(g) VALIDATE TRANSACTION
EXTERNAL AUTHENTICATION REQUEST CHALLENGE
COMPUTE AUTHENTICATION CODE (KAUTH)
RESPONSE AUTENTICATION (OK)
VERIFY RESPONSE (KAUTH)
(h)
(i) READ CP Req
DECRIPT CP (Kchif)
READ CP Req (ENCRYPTED CP)
(j)
DECRIPT CP (Kchif)
SEND TRANSACTION TO SERVER
SIGNED TRANSACTION
DISCONNECT
SIGNATURE
(k)

FIG. : 9

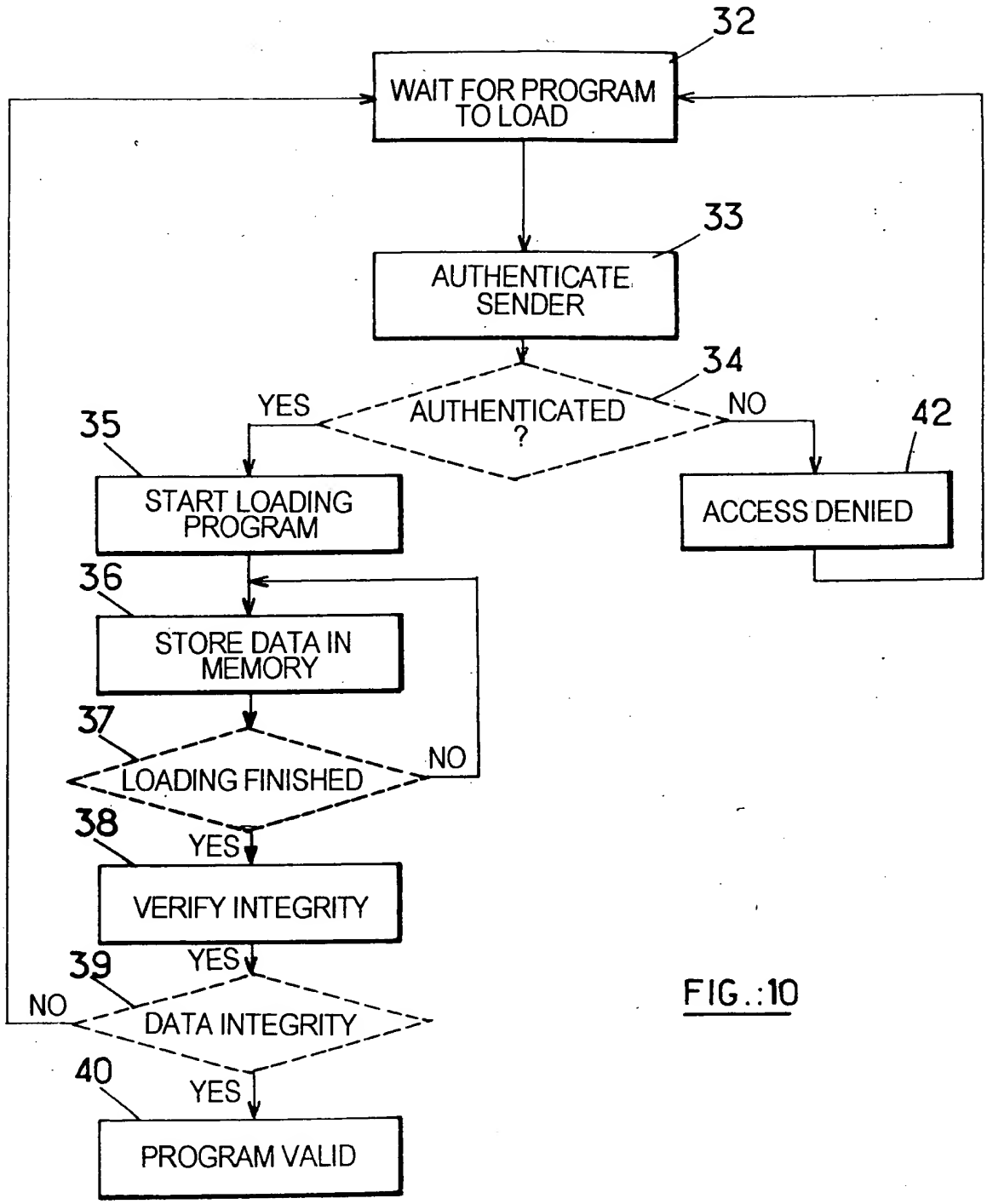

32
WAIT FOR PROGRAM TO LOAD
33
AUTHENTICATE SENDER
34
AUTHENTICATED ?
YES
NO
35
START LOADING PROGRAM
42
ACCESS DENIED
36
STORE DATA IN MEMORY
37
LOADING FINISHED
NO
38
YES
VERIFY INTEGRITY
39
YES
NO
DATA INTEGRITY
40
YES
PROGRAM VALID

FIG.:10